Smart Sovereignty and the Security of Society 5.0

An Explorative Study on the Challenges under the Technological Revolution, with Forecasting the Future

DOCTORAL THESIS

Presented to the Faculty of Management, Economics and Social Sciences at the University of Fribourg (Switzerland), in fulfillment of the requirements for the degree of Doctor of Philosophy in Management (Ph.D.)

by

Mohammad Aldabbas

From

Darayya, Syria

Accepted by the Faculty of Management, Economics and Social Sciences on December 19th, 2022, at the proposal of

Prof. Dr. Stephanie Teufel (First Advisor)

Prof. Dr. Marino Widmer (Second Advisor)

Fribourg, 2023

https://doi.org/10.51363/unifr.eth.2023.008

Acknowledgments

Writing a successful dissertation is in some way like winning a Formula One race. You need a good car (talent, material, and knowledge), good strategy (clear plan and suitable approach), good team (supervisors and mentors), and fuel (energy to keep going). Except that for the dissertation, I am racing against my weaknesses and the deadline of course. I am very lucky to have many great people around me. Thanks to their help I can finally see the checkered flag.

I am deeply grateful to my supervisors Prof. Dr. Stephanie Teufel, Dr. Bernd Teufel, and Prof. Dr. Marino Widmer from the University of Fribourg. Since I started my Master's studies, they have always been very supportive personally and professionally. I would like to express my gratitude for their ongoing support of my Ph.D. studies and research, as well as their patience and inspiration. Their advice was invaluable throughout my research and thesis writing.

I would like to thank Dr. Jean-François Emmenegger for enlightening me about the statistical analysis stage of the research. His kindness and patience helped me find the right path after I was lost.

Furthermore, I want to express my gratitude to Dr. Reinhard Bürgy, Dr. Toni Hürlimann, Francesca, and Vera for the great year I spent at the Decision Support & Operations Research Group at the University of Fribourg. I want to thank my colleagues from the iimt Kirstin, Yves, Mario, Julia, Virgile, and Melanie for the many memorable years of kindness, collaboration, and support.

My sincere thanks also go to my best friends Kinan, Ashraf, Mohammad, Majd, Musaab, Muhsen, and Danilo. Thank you for the years gone and the years to come of selfless friendship. You are brothers to me.

Last but not least, my sincere gratefulness goes to my loving wife Irina whose love and care were the fuel that kept me going, to my parents Khiro and Najwa, my siblings Hiba, Abdulrahman, and Zain, to my cousins Anas and Ahmad, to the sunshine of my life Elias, and to my brother Islam who lives on in my heart.

There are no words that can express my gratefulness for all these people and their continuous support throughout the entire time of writing this dissertation. Without them, there would simply be no accomplishment. Thank you.

Table of Contents

List of Figures

List of Tables

List of Boxes

List of Abbreviations

4IR	Fourth Industrial Revolution
ACF	Autocorrelation Function
AI	Artificial Intelligence
AR	Autoregressive
ARIMA	Autoregressive Integrated Moving Average
CHF	Swiss Franc
CPS	Cyber-Physical Systems
EPD	Electronic Patient Dossier
ETS	Error, Trend, Seasonality
EU	European Union
FAO	Food and Agriculture Organization
FSO	Federal Statistical Office
GAFAM	Google (Alphabet), Amazon, Facebook, Apple, and Microsoft
GCDD	Global Cyber Definitions Database
GDP	Gross Domestic Product
GDPR	General Data Protection Regulations
GFC	Gross Capital Formation
I4.0	Industry 4.0
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
iOS	iPhone Operating System
IoT	Internet of Things
IR	International Relations
MA	Moving Average
ML	Machine Learning
OECD	Organization for Economic Co-operation and Development

PACF	Partial Autocorrelation Function
PCC	Pearson Correlation Coefficient
PMCC	Product-moment Correlation Coefficient
QM	Quality Management
ROM	Read-Only Memory
SDGs	Sustainable Development Goals
SMEs	Small and Medium Enterprises
UN	United Nations
USA	United States of America
USD	United States Dollar
VAR Model	Vector Autoregressive Model
WEF	World Economic Forum
WHO	World Health Organization

1 Introduction to the Research Field

فَإِنَّكَ كَاللَّيْلِ الَّذِيْ هُوَ مُدْرِكِيْ

وَإِنْ خِلْتُ أَنَّ الْمُنْتَأَى عَنْكَ وَاسِعُ

The Arabic text above reads: “you are like the imminent night that will fall upon me, even if I thought that the distance between us is immense”. It is a verse from a 1400-year-old poem written by an elite poet known as Al-Nabighah[1] (the genius) after that his enemies forged a rumor against king Al-Numan who was so enraged and promised to kill him. In his poem, he was apologizing to the king and asking him for forgiveness. Fortunately for the poet, his begging was fruitful and the king forgave him. The link between this verse and our present time is that the waves of digitalization and technology will fall upon us eventually and change our society, even if we thought that they are far away.

“If the society and technology are to advance, research and theory must cope with rational and emotional intelligence and focus particularly on preserving the society for the favor of individuals.” Massey wrote this inspiring phrase when he investigated the role of emotion in social life (Massey 2002). The sentence is not particularly beautiful rhetorically, but its meaning and indications are.

This dissertation addresses the most important technology-driven security problems for the inevitable future smart society and the challenges triggered by massive dependence on advanced technology. As Massey noted, the individual's best interest will be the center of attention throughout this dissertation. Since the talk is about the future of human society, it makes sense to go back to history and understand how people in earlier societies understood and perceived security. However, why is that necessary? Simply to get a sense of how our understanding of security changes with time and will change in the future. Indeed, an accurate,

[1] Pre-Islamic Arab poet (died c. 604). See https://www.britannica.com/biography/al-Nabighah-al-Dhubyani for a short biography.

comprehensive answer to that question will not appear, but at the very least, an indicator about the development direction will come up.

Before elaborating on the matter, it is essential to refer here to the pH indicator, a chemical substance that changes the color of a solution when added. This process can determine the acidity or basicity of the solution. The name “indicator” describes very well the purpose of this substance. It is not a determinant, but it is just an indicator. The new color of the substance will expose the nature of the solution, but not its accurate pH number. So, the indicator's purpose in this dissertation's context is to sense the future understanding of security based on the evolution of security perception throughout the centuries.

This area of research is based on security but in an exceptionally innovative and novel approach. It is concerned with the future of human society from a human perspective. In other words, this research field has a touch of a human attribute. The research domain is about the future of human society, evolving with mass dependence on advanced and unprecedented technologies such as Machine Learning (ML) and Artificial Intelligence (AI). These technologies and their applications come with a price that society must pay. Just like when Thomas Savery invented the steam engine, the world witnessed a new ear, which was a turning point in the history of humanity. Naturally, the changes and the adaptation in society in all its aspects will need enough time. Various industries, social structures, policies, international powers, and much more will thrive to utilize these technologies best. The significance of successful adaptation and optimal utilization has the potential to disturb the balance of power amongst nations all over the world. According to the Global Competitiveness Report issued by the World Economic Forum (WEF), Switzerland is innovative and has kept its competitiveness very high (World Economic Forum 2020). The government and most companies in almost every industry are increasingly implementing more AI applications in their core structure. However, as mentioned before, this will come with a cost that people will have to pay before they can eventually adapt to the changes in every environment. The research field concerns societal security in the shadow of the downwards and the difficulties that carry this social transition. It is a vast field for research and very rich in sources for information because the technological waves are a technology Tsunami hitting every industry. The affected bodies within the society are not limited to the education system, job market, IT applications, social problems, psychology, operations research and optimization, healthcare system, taxation, mobility,

automobile industry, ethics and moralities, and many more. The future society will carry the name Society 5.0 or the Super-smart Society, as the Japanese like to name it (Hitachi 2020). This society was originally an initiative by the Japanese government. Society 5.0 is a concept of a new society that encompasses the endeavors to bring the ultimate value to the entire human society. The essential property of the future society is its mass dependence on technology. Society 5.0 is the latest in post-history human societies. It comes after the hunter-gatherer society, the agrarian society, the industrial society, and the information society. Society 5.0 symbolizes a super-smart, sustainable society with digital technologies built on digital infrastructures, platforms, and services (Cabinet Office 2018) embedded in every aspect and every fine detail to connect all the essential elements. The focus of this research field will be on the future of humans, the stability of the job market, the well-being of humans, the harmony in the interaction between man and machine, and other related matters.

Coherence is necessary for both the scientific process and results. (Brodbeck 2007) proposes a combination of critical rationalism and normative suggestions and provides a descriptive-empirical methodology leading to normative recommendations for action. The dissertation follows the discussed approach which is presented in Figure 1-1. Hence, for the entire dissertation all figures, tables, and boxes are the author's designs unless noted otherwise.

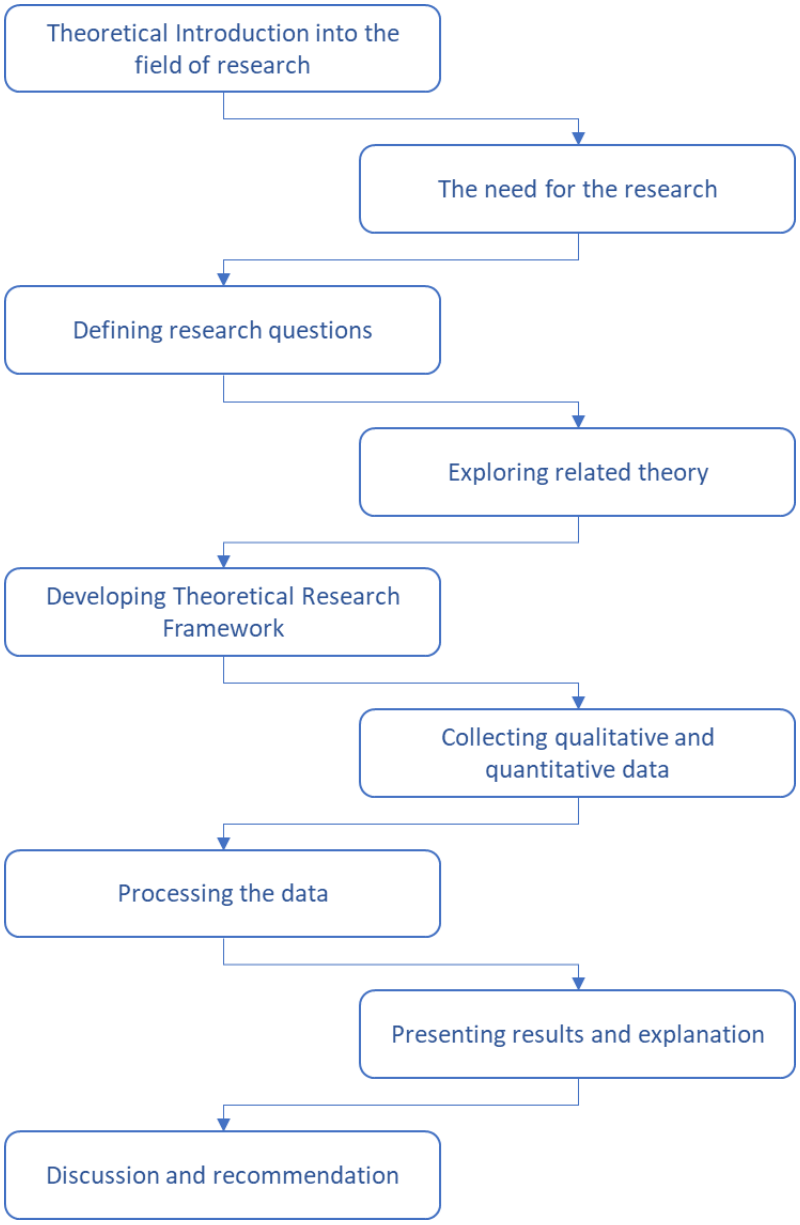


Figure 1-1: Scientific Research Approach for the Dissertation, based on (Brodbeck 2007)

1.1 Research Motivation and Research Question

We are witnessing a point of turning events that will cause the emergence of a new society. Massive waves of transformations are hitting the modern world where we live. This transition will change the world radically because digital transformation is relentless and inevitable, and significantly affects countless facets of our society in various fields. Changes will reach government administration, manufacturing structure, job creation, our perception of life, and even more private matters. Throughout this new age, and because of the increasing waves of globalization and due to the swift emergence and advancements of digital technology like the

Internet of Things (IoT), Industrial Internet of Things (IIoT), ML and Robotics, AI, and big data analytics (World Economic Forum 2019). All these technologies mean a significant alteration of the current human society. Our environment and values become even more complex with time (Bughin et al. 2017). The birth of the new smart society will carry many prospects to enhance life and increase the chances for a better future for everyone (Shiroishi et al. 2018). Society 5.0 will open doors for discovering new horizons in science in all its branches which is priceless. However, Society 5.0 will also bring novel problems that people will have to handle. Issues like lessening natural resources and global warming concerns (World Economic Forum 2019) will get more challenging to tackle. Growing economic fears, especially for third-world countries, are increasingly becoming complicated, and many other problems will either emerge (Aldabbas et al. 2020b) or develop new complications.

Consequently, the situation necessitates the development approaches of future Information. Engineers must redesign the Information and Communication Technology (ICT) to close the gaps between the desired position and the eventual status where the future society will be.

The purpose is to solve social difficulties efficiently and professionally, build a safer future for all individuals and sustain substantial economic progress (Weng et al. 2009; Acatech 2012). These matters provoke the problem of how we can guarantee that the future society will emerge in a way that concords with the desired social standards and ethics, and reach sustainable development for all society members.

After giving a general outline of the subject matter, the following questions are three main research questions presented in Box 1-1.

Box 1-1: Research Questions

- **Question 1:** "What are the most challenges that face Society 5.0 in the dawn of mass technology dependence? What security breaches accompany the technological revolution in the future?"
- **Question 2:** "How will the future society impact the lives of individuals? How will technology affect various aspects of life?"
- **Question 3:** "What is the sustainable security solution which reduces or negates the negative effects that accompany technology?"

This dissertation aims to provide answers and explanations for raised questions. The research will provide answers through the approaches presented in Table 1.1.

Table 1.1: Approaches to Answer the Research Questions

Question number	Approach to answering the question	The chapter containing the answer
(1)	Theoretical research will explore existing literature and extract the significant matters accompanied by technology that concerns society directly or indirectly. Additionally, the research will sense the direction and the potential of advanced technology to improve or deteriorate aspects like the quality of life in the future.	3.1 Theoretical Research: Challenges and Threats in Society 5.0 and Industry 4.0
(2)	Interviews: analyze interviews with experts in eGovernment, Small and Medium Enterprises (SMEs), and university education on matters concerning the future of Society 5.0 in Switzerland, challenges, and potential.	3.2 Qualitative Analysis: Experts' Opinions on the Future
(2)	Forecast: Forecast critical numbers in some selected domains of significant interest such as employment and healthcare to sketch the major shifts in Swiss society for the near future.	3.3 Quantitative Analysis: Forecasting Key Figures for the Future Society
(3)	Derive the solution and introduce "Smart Sovereignty" as a security shield for Society 5.0 in a way that Society 5.0 protects individuals and adheres to the principles of social ethics while placing the welfare of the people in focus.	4 Smart Sovereignty: Security Concept for Society 5.0

The research questions require complete thorough analysis. The analysis is the backbone of this dissertation, and the proposed solution is the core contribution. However, the analysis

needs a proper introduction so that the answers are put in the correct context. Therefore, introductory chapter 2 “Security and Society: The History and the Future” is necessary.

1.2 Aim and Outline of the Dissertation

This part will present the main purpose of the dissertation and the approach for this task. The outline of the dissertation will follow with the large picture of the research, and a clear explanation of the role each chapter plays.

Answering the research questions paves the path for the two major aims of this dissertation. The first aim is to offer a realistic prediction for Swiss society in the foreseeable future which is based on theoretical research, qualitative analysis based on experts’ judgment, and quantitative analysis based on historical data forecast to illustrate the practical implications of security matters on society and the lives of individuals and derive the most important technology-driven security concerns in the future society.

The second aim is to provide a solution for security problems. This solution is a new concept that will be used as a mechanism against future threats in the age of mass technology dependence, namely “Smart Sovereignty”. The research will make realistic recommendations to the government and the decision-makers in areas like policy, education system, and IT regulations to protect the future smart society in Switzerland as much as possible, and to push toward a sustainable super-smart Society 5.0.

The dissertation's outline covers the prerequisites for the research design as well as the goals and objectives. This chapter covers several phases of scientific inquiry as presented in Figure 1-1 and connected summary results. Figure 1-2 summarizes the thesis structure. The following paragraphs will examine the structure in more detail.

Chapter 1 has already presented the research field and the motivation for the research. This chapter also defined research questions.

Chapter 2 goes back in history to capture the perception of different human societies on security. Starting from the hunter-gatherer society to agrarian society, industrial society, and information society. The chapter explains how security requirements evolved and increased with time and with society's evolution as well. The understanding of security throughout

history will pave the way to understanding how security matters will change in the future Society 5.0, the Super-smart Society. It also explores different definitions of security in the literature, the contexts security is used, the different interpretations of this notion, and the shared basic elements for understanding security.

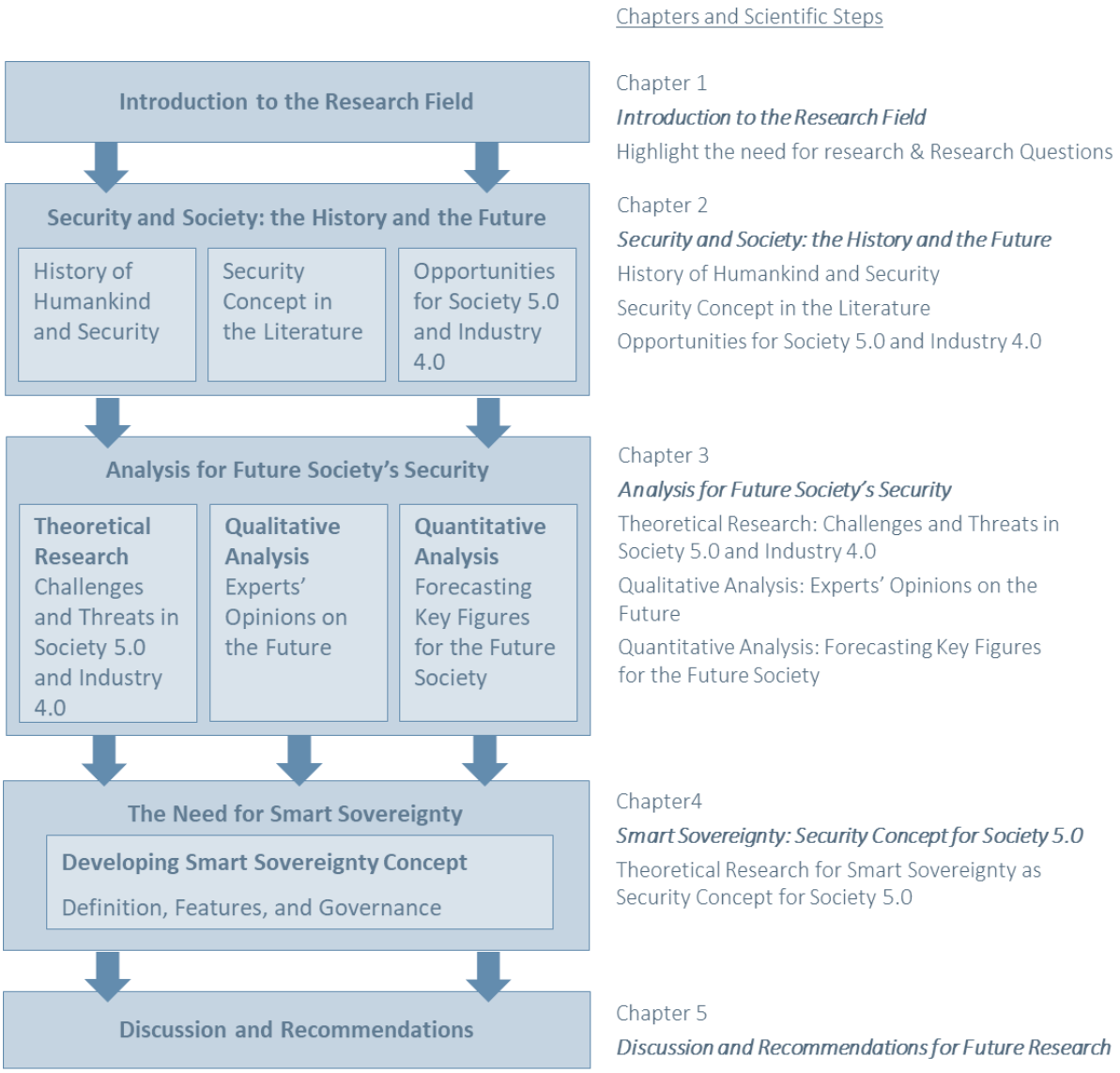


Figure 1-2: Outline of Dissertation Chapters According to Scientific Approach

Afterward, it defines "Societal Security" which is needed for Smart Sovereignty later. This chapter also explores different aspects of security like social security and national security with a special focus on digital and cyberspaces. Finally, this chapter presents some advantages and opportunities that cutting-edge technology will bring to the future. Since this chapter addresses three different topics, there will be page breaks between them for better reading.

Chapter 3 provides a comprehensive analysis of future challenges and risks to society using three approaches: theoretical research, qualitative analysis, and quantitative analysis.

The theoretical research addresses the problems and threats that accompany these technologies. It is also concerned with other social problems that technology will strengthen. Special attention is given to AI due to its importance to Society 5.0. Ethical problems are a hot topic for this dissertation. The author published a scientific paper which discusses these challenges (Aldabbas et al. 2020b).

The next step in this chapter is qualitatively analyzing interviews with professional experts from different domains of expertise. Since there might be a gap between theoretical research and practice, this step is necessary to get the complete picture or at least a more realistic picture of the matter on hand.

Only theoretical research and a qualitative approach might not be enough to have a general image of the future. Therefore, a quantitative analysis is needed to broaden the understanding of the challenges for the future society. The forecast in chapter 3.3 sheds some light on the effects of the progressive advancement of technology on Society 5.0 in Switzerland for some selected attributes. After discussing several forecasting methods and techniques, certain methods are selected and applied. This chapter presents the findings and discusses how they relate directly to our future which confirms the urgent need for acting. The author conducted a smaller forecast on a matter that is related to this topic. The forecast was published as a scientific paper (Aldabbas et al. 2021). It contributed to improving the knowledge for the main forecast in this dissertation.

The outcomes of chapter 3 give a strong signal that there is an urgent need for intervention, and it is best done by introducing Smart Sovereignty which is presented in the following chapter. The analyses in chapter 3 will be separated with page breaks for smoother reading.

Chapter 4 is the core contribution of this dissertation. It introduces the novel security concept for the future Society 5.0. The author built this chapter on the published paper (Aldabbas et al. 2020a) which introduced Smart Sovereignty and extended the research in this dissertation. This chapter starts by explaining the origins of sovereignty and how the concept emerged and developed with time. Afterward, the sovereignty concept is transformed into a more digital nature to adapt to the future. Later, this chapter explores the domains of application of Smart

Sovereignty and the way for an effective governance method, and how to sustain Smart Sovereignty.

Finally, **chapter 5** offers further discussion of results and the implementations in Society 5.0. The chapter summarizes the findings from other chapters, and emphasizes the most important keynotes. The objective is to offer study findings and, in doing so, to address the suggested research questions and provide straightforward answers. This chapter makes suggestions and recommendations based on the entire research. Lastly in this chapter, A prognosis for future research is provided, and so are the limitations of the dissertation.

2 Security and Society: The History and the Future

This chapter starts by telling the story of human societies and the evolution of society that happened throughout the years. Opening with the coexistence with nature in the hunter-gatherer society, to the development of irrigation techniques and establishment of settlements in the agrarian society, then the start of mass production with the invention of the steam engine in the industrial society, to the invention of computers and the distribution of information in the information society, until reaching Society 5.0 the super-smart society (Mavrodieva and Shaw 2020). All these topics are covered in chapter 2.1 History of Humankind and Security which also focuses on the meaning of security in all these eras, how people perceived security, and how security needs will evolve with society's evolution.

Next, chapter 2.2 Security Concept in the Literature explores the literature on security definition to provide a modern definition for “Societal Security” which is needed later for Smart Sovereignty.

Chapter 2.3 Opportunities for Society 5.0 and Industry 4.0 (often referred to as I4.0) wraps chapter 2 up by discussing new technologies, opportunities, and promises in the future super-smart society. Chapter 2 forms the environment and clarifies the context of this dissertation as Figure 1-2 illustrated.

This chapter does not provide a direct answer to any of the research questions, but chapter 2.2 introduces a definition that is necessary to answer research question number 3 (see Table 1.1 and Box 1-1). Nevertheless, chapter 2 gives valuable information and provides essential insights into the topic as presented in Figure 2-1 which shows the outlook for chapter 2.

Chapter 2 contains relatively long three subchapters, each of which covers its topic. For smoother reading, it is better to attach a conclusion to each subchapter directly rather than compacting a huge load of information into one conclusion.

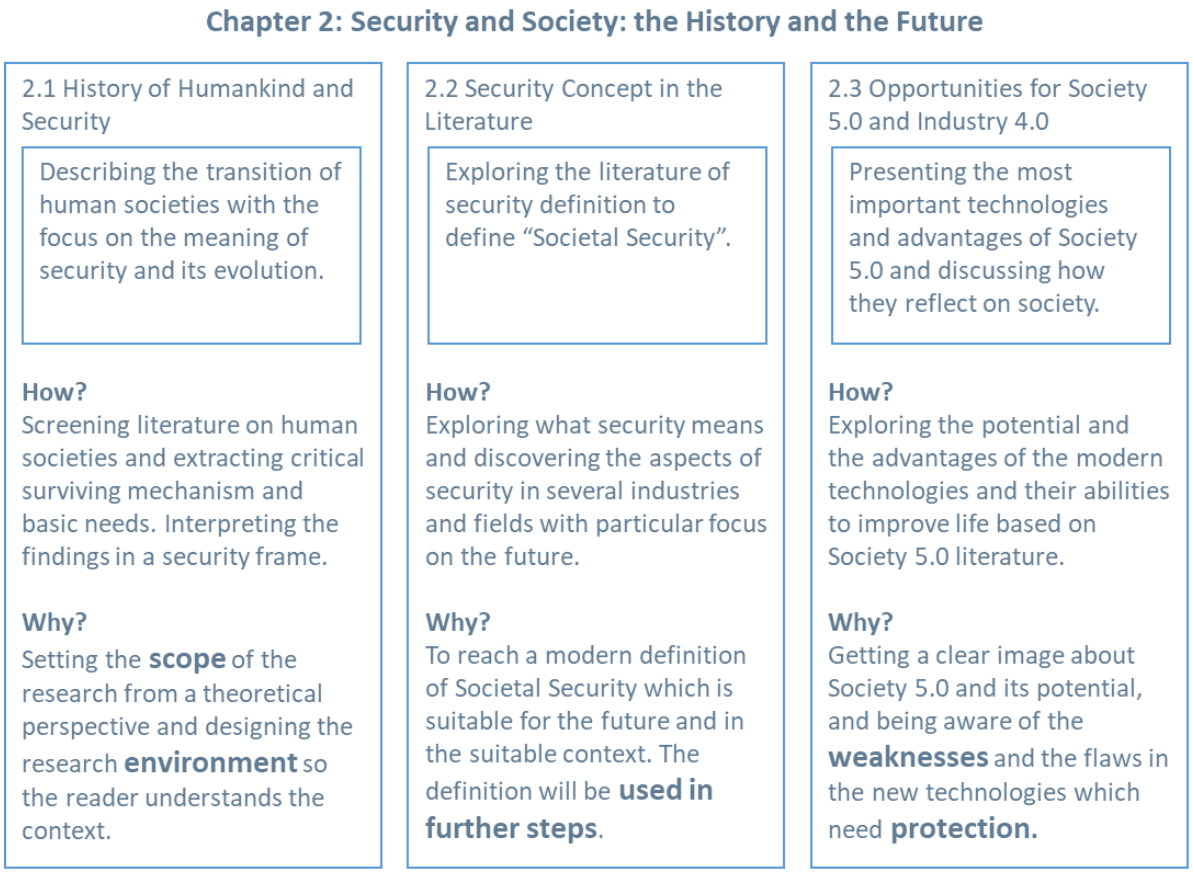


Figure 2-1: Chapter 2, Outlook

2.1 History of Humankind and Security

This chapter casts light on the history of human societies, the development of the security concept, what it has meant, and how security needs have kept evolving.

There are four distinguished societies throughout history: 1) Hunter-gatherer Society. 2) Agrarian Society. 3) Industrial Society .4) Information Society. The future brings the new Society 5, the super-smart society.

The timeline in the modified Figure 2-2 from (Aldabbas et al. 2020b) shows the periods each of these societies (co)existed.

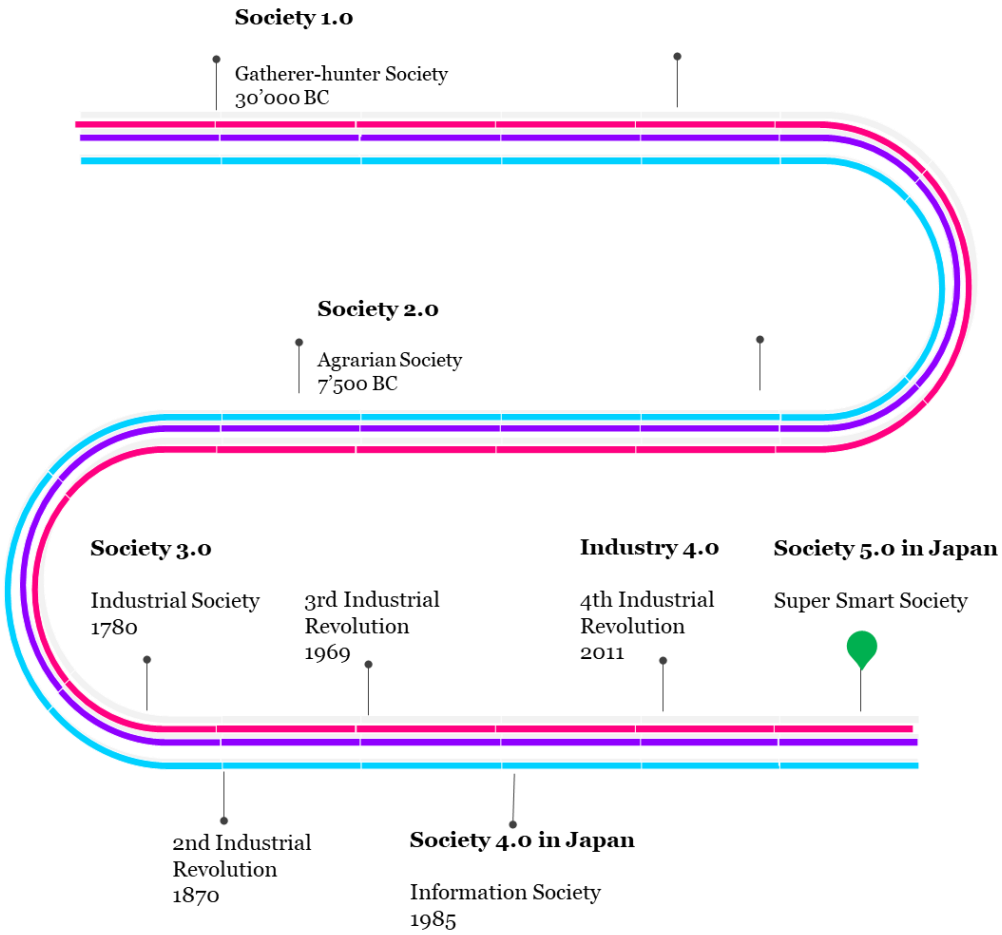


Figure 2-2: Human Societies Timeline, adapted from (Aldabbas et al. 2020b)

2.1.1 Hunter-Gatherer Society

Since the dawn of history and perhaps pre-history, humans have developed certain behaviors to defend and well place themselves against any danger. These behaviors are deeply inherited into the core of the societies from hunter-gatherers through today's modern society (Braithwaite 2005). The characteristics of these behaviors vary from one society to another and from geographical and historical locations to another.

There is much variability to be expected and several characteristics and adaptations for the hunter-gatherer society. The first society had different organizational patterns and different settlement strategies. They respond differently to problems and challenges. Understanding the hunter-gatherer society requires a decent knowledge of archeology and human science. The society that lasted the longest in the history of humanity was spread all over the world, in fundamentally different climatic circumstances and environmental conditions. The variations of locations are not limited to the Eskimos, whose lifestyle almost no longer exists, nor the

west coasts of California, or even to a 12000-year-old city that witnessed all ages like Damascus.

Many anthropologists make mistakes when they generalize their findings in one work field to the rest of the hunter-gatherer society all over the globe (Ember 1978). These prejudgments are inaccurate in many cases, and one should keep this in mind when reading about the hunter-gatherer society, especially since humans lived as foragers for almost 95% of the history of humankind (Hill et al. 2011).

The existence of human beings on earth goes way back in time. According to some scholars, societies emerged over 6 million years ago (Massey 2002). In comparison, others estimate a different number of years in the past. Doncaster (Doncaster 2019) argues that humans existed on earth 2 million years ago. There are many different theories and estimations about when the starting point was. Nonetheless, many archeologists come together closer when they estimate the beginning of cultural development and the formation of the first society: The hunter-gatherer society.

Before the appearance of a hunter-gatherer society, their antecedents depended on the leftovers that predators left behind. (National Geographic Society 2019). The hunter-gatherer culture of living was the only developed way to survive. This era lasted until 11 to 12 thousand years ago. The main lifestyle is based completely on hunting animals, fishing, gathering food, and substances like honey and vegetables. (National Geographic Society 2019)

The hunter-gatherers had to rely on mobility to survive because they did not yet depend on agriculture. Their lifestyle needed accessibility to large lands to find the substances. Consequently, they were not able to stay for long terms or establish settlements. They lived in groups not larger than 100 people and mainly consisted of families. (National Geographic Society 2019). This society also depended on the exchange of all kinds of resources, such as materials and information. Usually, the transformation was directly from one human to another. Society, from the perspective of socioeconomic, according to some researchers, is a system that initiates and preserves an endless amount of energy and materials to produce and sustain its components (Musel 2009). The flow rates regularly reduce from families to larger groups in accord with the effects of kinship and mutuality on the costs and benefits of exchanges among larger groups with reduced contacts (Hamilton et al. 2007b). Production of material was not unknown in the hunter-gatherer society. However, the manufacture and

consumption of material positions were minimal and restricted mainly to perishable nourishments and tools (Burgess 2010). Mobility, traveling, and relationships with other groups were essential for society to secure its needs for substances and the exchange of material and information.

With the arrival of the agricultural revolution around 12000 years ago, many groups of gatherer-hunter deserted their practices and established permanent settlements. Bigger groups and populations evolved. However, many practices of the hunter-gatherer continued until the modern age in parts of Europe and the Americas (National Geographic Society 2019). Nevertheless, in the last five centuries, the remains of hunter-gatherer societies declined drastically. Today, only a few groups still practice hunting and gathering in their traditions as the main means to survive.

Anthropologists at the beginning of the 20th century believed that hunter-gatherer societies shared everything they owned with other groups, even lands. Later, however, shreds of evidence of territoriality amongst these societies emerged. Contrary to dominant belief, the territorial boundaries seemed strict between groups, and any violation of others' land could lead to a deadly fight (Baker 2003). Therefore, land security was vital in the hunter-gatherer society as it provided essential resources for survival. Nevertheless, land usage was not exclusive to the group that owned it. Other groups were sometimes allowed access and benefit from the territory (Baker 2003). Another means to secure the society against undesired combats with other groups was to grant or allow access to other groups to the owned or possessed land.

The hunter-gatherer society is a part of complex ecosystems. These systems depended on different levels of exchanging materials within the environment. They collect resources from their environment to meet their essential needs of nutrition. They also adjust the size of their groups as a response to the variations in locations and available resources because resources are rare and dispersed (Binford 1980; Hamilton et al. 2007b). The reason for the number adaptation is that the required space per individual to reach food security decreases in large populations (Hamilton et al. 2007a), which introduced a sort of economy of scale where the efficiency of food gathering increases with the size of the society (Hamilton et al. 2007b). Therefore, it is possible to assume that the security of the society was inherent in meeting basic

metabolic and material requirements, and it is correlated with the size of the landscape and the size of the group.

Marriage has been a fundamental issue since the first modern humans. The hunter-gatherer society enjoyed a level of complexity in society that has a deep history of regulated marriage. Marriage is necessary for economic and social factors. It played an important role in alliance with other groups (Walker et al. 2011). It brought stability and security to many aspects of society. The exchange of mates and resources enhanced the complexity of society and allowed collation and alliances among different groups and communities. (Walker et al. 2011). Marriages were also a security factor for the hunter-gatherer society, as they strengthened the relationships between tribes.

Achieving food security (see chapter 2.2.1.5.1) was always challenging for hunter-gatherers daily (Ong and Kim 2017). They encountered many difficulties providing for the groups. Evidence that even wild edible plants were considered vital food for poor families (Delang 2006). The wild edible plants were essential for some of the hunter-gatherer societies – in the Philippines- not only as food but also as a social and cultural expression of the group (Ong and Kim 2017). In the later agrarian society, wild plants remained important together with cultivated cereals, especially in the early phases of the agrarian society (Whitehouse and Kirleis 2014). The role of wild edible plants in household food security is very visible.

As explained by evolution and ecology theory, hunter-gatherers tend to mark their territories based on rational choice. They select a territory when the advantages of excluding other groups exceed the costs of defending the territory (Tushingham and Bettinger 2019). They store food and materials in these territories and must defend them. However, only if the cost of defending is lower than the cost of losing this storage (Tushingham and Bettinger 2019). The security of this storage is important to society because storage contributes to settlement and population growth. Storage alters society's population-territory size dynamics (Freeman and Anderies 2015).

Food security, which means having enough food and water, is important and needs protection from harmful predators, especially in a brutal environment. Otherwise, the species will have to encounter extinction. The groups had to develop socially to solve the issue, and the tendency to exchange materials and resources became common (Braithwaite 2005), illustrating the importance and power of social life in the hunter-gatherer society. Not to underestimate, the

hunter-gatherers' existence relies on their partnership and coalition (Braithwaite 2005) as one group and one society.

The social structure of the hunter-gatherer is complex and unique, as mentioned earlier. According to (Hill et al. 2011), there is evidence that most individuals in residential are not blood-related groups, which means large interaction networks with other groups. These big social networks explain why hunter-gatherers developed capabilities for social learning and created cumulative culture.

There have been stereotypes until the late 1960s of the last century that hunter-gatherers were at their best “noble savages” and “brutal” otherwise (Lomas 2009). Later, anthropologists’ discoveries revolutionized these badly perceived hunter-gatherers, and data collection and evidence showed that they were smart and peaceful people (Lomas 2009). They tend to show extensive support and cooperation with other group members (Hill et al. 2011), which does not imply conflicts and wars between tribes and groups. However, the cause of these conflicts is natural cause due to competition over resources like land and substances (Gat 2000). Many types of conflicts were resolved peacefully. Social and cultural pressure also played a role in solving conflicts nonviolently (Lomas 2009). That is another form of the importance of social control for the security of the hunter-gatherer society.

2.1.2 Agrarian Society

The transition to society 2.0

In the middle east and north African regions and approximately 12’000 years ago, the first signs of permanent settlement for groups of hunter-gatherers were born. Well-organized peoples of hunter-gatherers established a new lifestyle and focused on limited vital types of plants and animals as the main source of nutrition (Helms 2004). Later, this Neolithic revolution or agricultural revolution transition in lifestyle and subsistence from foraging to farming was known as the Neolithic Demographic Transition (Bocquet-Appel 2011). The domestication of animals and the development of modern agriculture took place in a new and significant way for the first time in history. Later, agriculture spread out, advanced, and matured independently in the rest of the world (Helms 2004). This shift caused a significant rise in human populations, approximating an increased fertility rate of women to two births.

Moreover, this unique demographic change played a central role in restructuring human history (Bocquet-Appel 2011).

After living over 2 million years as hunter-gatherers, humans started to settle and work as more modern farmers in seven or eight regions all over the globe (Bocquet-Appel 2011). Archeology digging in Mesopotamia revealed signs of wheat cultivation and pottery made by hand that go back about 10'000 years in time. The domestication of sheep and goats began in the Fertile Crescent and Turkey approximately 10'500 years ago (Doncaster 2019). These transitions happened at nearly the same time, between 8'500 BC and 1500 BC (Bellwood 2005). Nevertheless, a few regions still live as hunter-gatherers, as noted before. The world's population during the birth of an agrarian society is very hard to estimate. An approximation suggests that the population in 10'000 BC was between one million and 10 million, with high uncertainty (Pala et al. 2012).

The transition process from hunter-gatherer to agrarian society varies from one region to another and from one continent to the other. There is no consensus on the mechanism of this transition. For example, the emergence of agrarian society in south Scandinavia and northern parts of Germany was subject to debate for over a century (Sørensen and Karg 2014). There are mainly two hypotheses: the first suggests that migrating agrarian societies introduced agriculture in the region. The reasons for these transitions remain unknown, but assumptions attribute them to better climatic conditions and access to resources, especially in flint. The other hypothesis proposes that agriculture was adapted by the population gradually. However, in this case, many scholars prefer the gradual adaptation of agriculture (Sørensen and Karg 2014). That shows the complexity of determining the mechanism of social transition all over the world, especially bearing in mind that up to this day, several regions still live as hunter-gatherers, as noted earlier.

A big demographic shift happened after the settlement of the hunter-gatherers, mainly in the regions of the Levant, in north and south China, New Guinea, and Ethiopia, and eastern North America, Mesoamerica, and South America (Bocquet-Appel 2011). The demographic shift was due to the increase in fertility pushed by a better and healthier lifestyle in terms of nutrition and better energy balance (Valeggia and Ellison 2004). The food gained from farming is high in calories. Mainly wheat, lentils, and rice, instead of the low-calorie common food in the hunter-

gatherer society, i.e., wild animals. In addition to the decreased energy spent on moving and carrying infants (Bocquet-Appel 2011).

Commitment to agriculture needs stability and security in society, not only physical but also social security. Without the safety of society and the solidness of the social systems, agriculture will not endure. Hence, there is evidence in northern Europe that despite the dominance of agriculture, it was in many areas augmented by fishing and hunting (Sørensen and Karg 2014).

Agriculture needs commitment (Bender 1978) and technology to prosper. The understanding of the agricultural society cannot be complete if it is attributed only to technological development and demographical growth. Many researchers gave the attributes of commitment and technology much focus in their work. However, the social structure was paid as much attention (Bender 1978) at least until the end of the twentieth century. Many historians minimized and underestimated the importance of social factors (Postan and Hatcher 1978). To have a general overview of the security matters of the agrarian society, all three components, i.e., technology, demography, and social structure, will be examined.

Agricultural technology and demographic expansion depended on the social structure, according to (Bender 1978), after examining tribal systems in anthropological frameworks. The social properties of a tribal system can generate increasing demand for production. Production demand mandates a commitment to agriculture (Bender 1978). The earlier hunter-gather society showed the importance and strength of family relationships, with a less but strong connection to the group, noticeable through the exchange and transformation of materials and information (Hamilton et al. 2007b). The social structure of the hunter-gatherer was complex (Hamilton et al. 2007b), a similar characteristic of the agrarian society.

Social structure in agrarian society

In the regions where hunter-gatherers lived and later transformed into agrarians because of migration, there remains a complex question that can affect the region's social structure. The question is: what happened to the residing hunter-gatherers? In the example of southern Scandinavia (Sørensen and Karg 2014), there are two possibilities: the hunter-gatherers became farmers after one or two generations. The other possibility is a cultural dualism between farmers living in inland areas and hunter-gatherers living near the coasts and the lakes. The agrarian and hunter-gatherer societies co-existed, with the hunter-gatherers

adopting new tools and some of the agrarian cultures in addition to cultivation. Both explanations are possible, but there is a tendency backed up by archeological pieces of evidence to favor cultural dualism (Sørensen and Karg 2014). It is possible, therefore, to assume that the social transition from hunter-gatherer to agrarian society is a complex continuous process. The social structure's importance and values of the social structure transferred from the hunter-gatherer society to the new agrarian society.

Archeological evidence in Sweden showed that in the preindustrial agrarian society, there was a tendency to use remains of humans and animals to perform magic porpoises that are believed to bring safety and prosperity, especially in the iron age (Paulsson-Holmberg 1997). These beliefs were possibly transformed from the earlier hunter-gatherer society by their descendants.

In the latest stages of agrarian society, the importance of agriculture continued to be the backbone for many countries together with the advances in technology, the changes in politics, and the spread of democracy. Agriculture enjoyed different importance in the US in the 18th century. Kelsey (Kelsey 1994) explains that the term agrarianism refers to a philosophy identified by Thomas Jefferson. It had a significant impact on Americans' vision of agriculture and most American political and social movements since the early days of the United States of America. The image of agrarianism reflects that farm life results in good people and that farmers tend to be democratic, truthful, and self-determining, in addition to being stable politically more than the city inhabitants. At the same time equally, the meaning of this philosophy implies that the rest of the nation owes farmers for living a such hard life with very low income in comparison to others and the little control they have over the worth of their efforts, and without the farmers, the democracy would not prosper in the nation. This strong perception of agriculture served as the cultural identity of the Americans. The safety of farmers, the security of the occupation, and the prevention and intervention in case of a work injury on the farm, whose rate was very high a hundred years ago, were always important for policymakers and society. In general terms, the safety of farmers and the security of agriculture were significant not only for food production and nutrition but also for political stability and the general security of the nation.

Kelsey (Kelsey 1994) explains the strategy and the policy to protect farmers and agriculture. The public in the US in the 18th century was aware of the high rates of injuries and death on

farms. The owners of farms tried to secure several important issues and push for legislation to protect them at the taxpayers' cost. Despite the importance of agriculture and the perception of its vital role in the country, safety programs by the government could never go smoothly and without huge debates. Here are some of the security points that mattered most:

- The rates of injuries and death on farms need to be reduced. However, no agreements were achieved on how to respond because the perception of the safety of agriculture is not the same for all people, and the responsibility to respond is differently perceived. The counter-argument against farmers is that it is in their interest to be safe, and they must make their environment safer (Lee 1998).
- The target population that needs a safety program was not clarified, and the description of people on the farm was ambiguous. Farmers, partners, owners, employees, operators, and family members exist. The involvement of all these people was always a question for debate. There was also the differentiation between farms by size, economic condition, and population size on the farm. The issue is that adapting agricultural safety programs in a homogenous method to all farms will qualify rich farmers for high-cost programs (Kelsey 1994).
- One question that remains unanswered and very broad is who should take over the costs of agricultural safety. Many different costs can be identified: certification of machines to be used, does everyone who has access to resources such as land, water, or labor qualify to be considered a farmer and benefit from the program? Has anyone with sheep on his land the right to get money to practice his hobby?

  Usually, due to the strength of the image of agrarianism, the default answer will be that the taxpayers have to pay for the safety program. Nevertheless, this remains unjustified and unexamined, especially since it is unknown where the line of taxpayer support stops and where the line of the farmer bearing his own cost begins (Kelsey 1994).

Security in agriculture takes a new dimension that never existed before, resulting from social development and political movements, even if the public overvalues agrarianism because of political and social movements' campaigns.

Food security in agrarian economies suffers from several issues (Holden and Ghebru 2016): decentralized and dispersed food production, unavailability of good infrastructure, relatively costly transportation, and perishable vegetables. All these factors limit the inputs in food

markets and make security a challenge for households. According to countless studies, tenure security is another essential issue that plays a major role in the economies of agrarian societies (Holden and Ghebru 2016). Tenure security is "the legal right to continue living in or using a building, land, etc. that is rented from the owner" as per Cambridge Dictionary (Cambridge 2020).

By the 12th century, several big countries were formed, and the economy depended heavily on agriculture which prospered in England and several European countries. However, by the end of the 13th century, this prosperity started to decline, and the recession spread in many regions causing agriculture to be a huge problem (Campbell 2005). That can cause some new security issues for society. Such an economic crisis did not exist in the earlier days of the agrarian society with such a huge impact. Economic security became a serious issue for society. During this crisis, the population started living in an utterly hard situation and became more prone to crisis (Campbell 2005). There were many attempts to explain this case of agricultural problem in England. (Campbell 2005) suggests that part of the problem was a crisis within the feudal system between the landlords and the tenants. This case sheds some light on the new level of complexity in the agrarian society where social, legal, economic, and agricultural systems must work in harmony to avoid crises and recessions. The reader can refer to (Campbell 2005) for more insight on this topic.

2.1.3 Industrial Society

The industrial revolution is one of the most written and documented shaking events that ever happened in the history of humankind. Many studies addressed the transformation from an agrarian society to an industrial society from several perspectives, i.e., social, economic, and historic (Musel 2009). The industrial revolution came with the mass migration of labor from suburbs to the cities, and the secular ideology, universal liberty, and equality matter raised with the French revolution. All these major events changed the world fundamentally and created the modern world as we know it today (Sevilla Guzmán and Woodgate 2013). The industrial revolution did not happen only one time as a major event. It rather went through four distinctive phases. The first industrial revolution was the dawn of mechanical production and began around 1760 with the arrival of the steam engine. The engine was implemented in every sector, from agriculture to textile manufacturing. Societies were completely dependent

on farming. The first revolution shifted the center of societies from farms to factories (Schwab 2016). Agricultural production developed and grew faster in the 19th century in Britain after the industrial revolution, with some dependency on imported nutrients (Sevilla Guzmán and Woodgate 2013). The second industrial revolution began at the beginning of the 20th century thanks to electric-powered mass production. It was the age of science, too, as science was implemented in factories. Compared to just 6% in 1800, approximately 40% of Americans inhabited cities by 1900. New inventions like electric lights, the radio, and the telephone changed how people connected and interacted with each other with the rise in urbanization (Schwab 2016). By the start of the 1960s, electronics and IT were massively used to achieve further automation in manufacturing, which was the sign of the third industrial revolution. This revolution was digital. It brought semiconductors in the 1960s, mainframe computers, personal computers in the 1970s and 80s, and the internet in1990s (Schwab 2016).

Main security issues revolve around job security, migration flow, data security systems, and international security. Food security continues and is still a problem that faces governments all over the world. Food security was always a dispute between regulators, politicians, and thinkers (Zabel 2018). International security comes from inequality, social trust, and violence. However, these matters are not given sufficient discussion in the public domain despite their importance to society (Schwab 2016). Data rights and protection laws were highly fragmented despite the internet network's international nature and the expanding global economy. While many other jurisdictions still had weak regulations or none, those governing the collection, use, and sale of personal data were well recognized in Europe. Big internet operators could infer more information than was supplied by users because of the aggregation of large databases (Schwab 2016). Security problems kept growing like a snowball with the advancement of human societies. There is no evidence that they will not gain more complexity in the future. All signs suggest that future security issues will become more complex, especially due to modern technology.

2.1.4 Information Society

The notion of the information society can be confusing due to different naming in different geographic locations. In Europe, the information society overlaps partly with the third industrial revolution. However, in Japan, the information society is recognized as distinct

evolution of human societies. It emerged in Japan in the early 1960s (Karvalics 2007). In English literature, different terms, such as post-industrial society and the white-collar revolution, were widely used to describe the newly emerging social-economic society (Karvalics 2007). However, naming societies and their phases have no global consensus. For example, the expression “post-industrial society” first appeared in 1914 in England. Then it was revived in the US in 1958, and by the end 1960s, it evolved in France as (Karvalics 2007) explains. This tendency for nations to opt for different naming for their societies continues today. Therefore, one should not read too much into the naming. More focus should be on the timeline when these societies evolve and decline and on the technologies being used and applied.

Besides the security problems in the industrial revolution society, cyber warfare is one of the most significant concerns for the information society. As with land, sea, and air in the past, cyberspace was increasingly used as a battlefield. Any future confrontation between decently sophisticated actors would almost certainly involve cyberspace since no modern adversary would be able to resist the urge to interfere with, confuse, or destroy their enemy's sensors, communications, and capacity to make decisions (Schwab 2016).

This society is massively dependent on information, which calls for new weaknesses within the system that humans cause. Information security management mostly disregards the human dimension. The major focus is on technical and procedural measures. The user is regarded as a security enemy, not a security asset (Schlienger and Teufel 2002). Therefore, it is necessary to shift from regarding humans within the system as an enemy to seeing them as allies (Aldabbas et al. 2017; Schlienger and Teufel 2002). Instead of starting with the technology, designing a security process and putting it into practice should focus on the personnel involved everywhere within the society on a micro level. Consequently, society’s total security level may be significantly raised by combining technology and human awareness (Schlienger and Teufel 2002).

2.1.5 Super-Smart Society, and Industry 4.0

Industrial revolutions occur as a result of the fast growth of knowledge, technology, and social life. With these revolutions, new options, chances, and benefits emerge for institutions or organizations on an economic, social, and demographic level (Calp and Bütüner 2022). The transformation in humanity's society is coming in only a matter of time. The next society will

be called the super-smart society or Society 5.0 in Japan and aims to enhance Japan's environment for innovation (Holroyd 2022). The society is called Industry 4.0 in Europe, Smart Cities in Asia, and Industrial Internet in North America (Fukuyama 2018). Figure 2-3 (Fukuyama 2018) shows the worldwide digital transformation which forms the pillar of industrial policy.

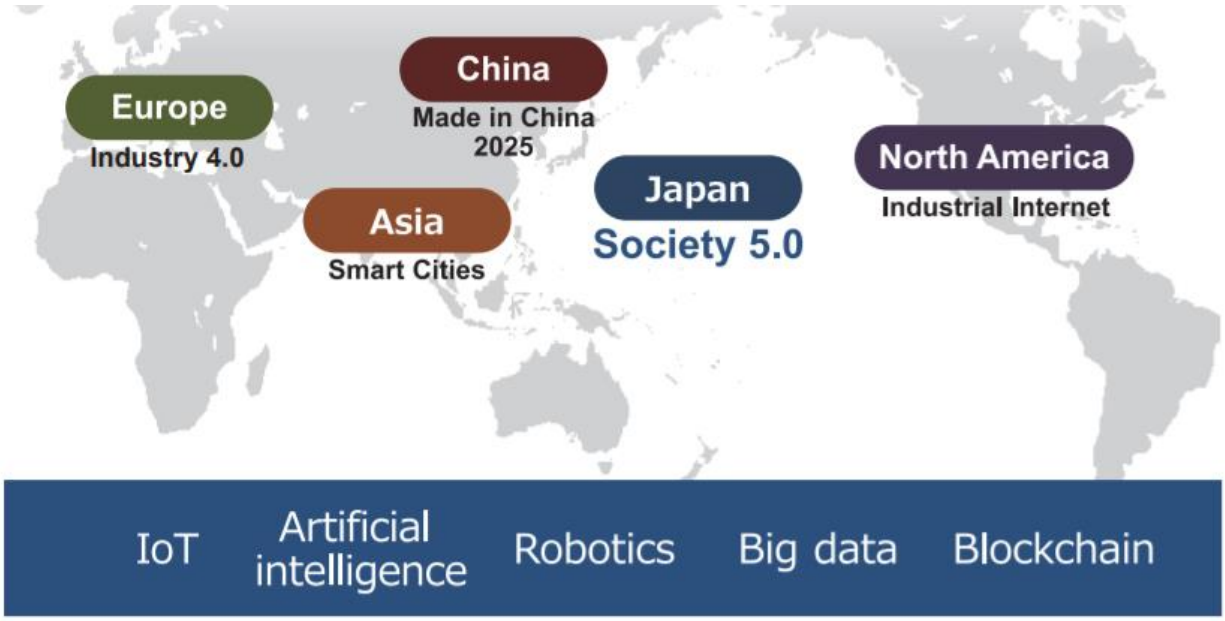


Figure 2-3: Digital Transformation in the World (Fukuyama 2018)

The core tools and technologies for the 4IR and Society 5.0 are not limited to the IoT, big data, AI, deep learning, quantum computing, autonomous robots, cloud computing, cyber-physical systems (CPS), and blockchains (Holroyd 2022; Fukuyama 2018; Mora et al. 2021; Calp and Bütüner 2022). These are the formers and shapers of our future as humans and will greatly influence the direction our social life will develop (Fukuyama 2018). Each wave of change carries contesting challenges for society to adapt, but luckily it brings prospects for prosperity. Society 5.0 requests that all public and private sector actors change their course from one that places a heavy focus on commercializing technology to one that is more inclusive and puts society first (Holroyd 2022).

The super-smart society in Japan is still in its infancy. Although speed and effectiveness in innovation projects are a cornerstone of the government's work, it is difficult to foresee a speedy transition (Holroyd 2022). Society 5.0 is not an exception in terms of obstacles and problems to security. Nevertheless, plenty of advantages and progressions are expected as well. People need to be well-equipped and prepared for what is coming. Above all, they should

be armed with knowledge and awareness of the danger. Otherwise, the consequences will not be in their favor.

For more reading on Society 5.0, the reader is referred to (Calp and Bütüner 2022; Fukuyama 2018; Holroyd 2022; Hitachi 2020; Cabinet Office 2018; Salgues 2018; Shiroishi et al. 2018; Deguchi et al.).

2.1.6 Conclusion

Table 2.1 presents a brief comparison of security needs throughout the history of human societies. Most of the basic security challenges since the hunter-gatherer society still exist today. Aside from criminology, wars, plagues, and natural disasters, the points noted in the table are the most significant for society. For Society 5.0, a separate chapter 3.1 is dedicated to this analysis.

Table 2.1: Security and Challenges for Human Societies

Society	**Security matters and challenges**
Hunter-gatherer society	Safe living spaces, basic metabolic and material requirements, food and water, safety from harmful predators, relations with other groups through marriage and collation
Agrarian society	Injury rates and death on farms, population size on farms, economic struggle, food security, transportation costs, safe housing, tenure security, recessions, social classes, and injustice
Industrial society	job security, migration flow, data security, international conflicts, food security, social justice, data rights protection
Information society	Cyber security, data protection, information security

Security needs have changed throughout history, and security problems also changed human society. It started with the basic needs that Maslow summarized in his famous pyramid. However, today a skyscraper is probably needed to accommodate all security fears. So much is required today for humans to feel complete or mostly safe.

A look at the future

In Japan, the Council for Social Principles of Human-centric AI was formed, consisting of various academic groups, public institutions, and corporate sectors. The Council recommended the implementation of several principles, including: (1) a human-centric principle, which states that AI should not interfere with fundamental human rights established by legislation; (2) a principle of education, which states that people will have an equal opportunity to learn and use AI technology safely and will receive adequate information on the benefits and risks of using such technology; and (3) a principle of transparency. (4) the concept of privacy protection concerning the use of personal data, which should not impair individual freedom and equality, (5) the principle of security (cyber security), (6) The concept of fair competition, which tries to avoid data monopoly, (7) The principle of fairness, accountability, and transparency, which is free of segregation and bias, and (8) The principle of innovation, which encourages collaborative efforts among many players. While the principles reflect the need for equality and a humanistic attitude to all of society, they do not emphasize the involvement of excluded groups in decision-making. For example, members of civil society groups do not appear to be represented on the Council (Mavrodieva and Shaw 2020).

2.2 Security Concept in the Literature

The difficulty with the definition of security in classic and modern socio-political science is that it was investigated either too specifically with many details or too generally (Grizold 1994). Many concerned parties from all disciplines have made it impossible to delineate a formal or official definition of security throughout the years.

The definition of security has always been a target of many studies. However, there is absolutely no overall accepted definition of security in the literature, especially in defining security as a general term and in a general sense (Collard et al. 2017). Security in its nature is multidimensional, but in practice, it varies (Brooks 2010) depending on the environment and the context that it is in use. That is why finding a generally accepted definition of security is so difficult. Before diving into the long history of humankind and the relation and connection to security it represents to all human societies, there is an imperative need to understand the concept and the sense of security.

Originally, all social activities throughout the history of human societies and the interaction with nature connect to the notion of security for humans. Security is one of the basic absolute necessities for human beings and is a precondition not only for fundamental daily activities but also for survival in the first place. In the well-known Maslow's hierarchy of needs, safety needs are in the second lowest place in the pyramid. Only second to primal physiological needs like food and water, as seen in Figure 2-4 (Mcleod 2007).

Figure 2-4 Maslow's Hierarchy of Needs (Mcleod 2007)

Security can be considered at the heart of every development and entails intentional and purposeful human attempts to establish a modern society with a state of safety (Grizold 1994). However, as discussed in this paragraph, the notion of security is explained as the absence of threats, which makes it very general. Grizold (Grizold 1994) based his definition on conscious efforts to create a state of security as a necessity for civilization incorporating the importance of culture for society and not disregarding national and international aspects of life. He defines security as a "conscious human endeavor to establish the state of security through social activity organized into an adequate system". Grizold (Grizold 1994) explains that he defined security as an essential component of society and seeks to achieve a balanced state in several fields such as physical, spiritual, cultural, and psychological, not only for the individual but for the community as a whole.

Some researchers define security as "the absence of another state," like threats and danger. Some researchers define security as defending or delaying that undesired dangerous state like Oakes does (Oakes 2009) "Security is the process or means of delaying, preventing and otherwise protecting against external or internal dangers, loss, criminals, and other individuals or actions that threaten to weaken, hinder or destroy an organization's steady state".

Modern definitions for security like Merriam-Webster's dictionary provide several definitions and a clear concept. Security is "the state of being protected or safe from harm" (Merriam Webster 2020b). The dictionary explains more states for security. It describes security as the quality of being secure from danger, freedom from fear or anxiety, job security, and other security matters. This variance of approaches shows the wide range of the definition of security and the difficulty of selecting a generally accepted understanding of security. Nevertheless, selecting a definition of security that will accompany the reader through this topic is an important mission.

To define security, one must understand what needs securing at the beginning. Let that be objects, values, or people. Then, from what are we securing these things? The risks and threats need defining. Afterward, who is initiating these risks? Is it an outsider to the environment that needs protection? Or are there insiders that create chaos? The complexity of reaching a definition is apparent in the difficulty of answering all these questions. Moreover, if the domain of research or science changes, then so do the questions. Likewise, the answers and the definition will change as well.

Despite the difficulty of reaching a definition for security, several mutual keywords appear in many of the definitions found in the literature, which provides at least a general popular understanding of security and what it can represent in a certain environment under certain conditions.

A dive into the literature for security definitions should help compose a scientific understanding of security. Brooks (Brooks 2010) reports that security in a traditional definition is providing private services to protect people, information, and assets for the safety of individuals and society. There is a strong correlation between defense and security as both deliver protection. However, there are troubling differences between these two industries (Brooks 2010). One should remember that the notion of a defense often comes together with police and military organizations.

A more applicable definition by Baldwin (Baldwin 1997) presents the following reformed definition for security “a low probability of damage to acquired values”. Baldwin states that two specifications are needed to define security in its most basic form. 1. Security for whom? And 2. Security for what assets? Baldwin describes a condition with a low probability of damage occurring. Consequently, this definition is static because a given probability of damage occurring is tied to a specific point in time. In other words, this definition is a snapshot.

A big advantage of Baldwin’s definition (Baldwin 1997) is that it is suitable for comparing different safety states. These comparisons may involve the same assets at different points in time or different assets at the same time. From these comparisons, one can conclude how the probability of damage occurring develops over time or which assets are more likely to be damaged at a given time. It is therefore conceivable that Baldwin's definition could be usable as a basis for safety comparisons.

The following example illustrates how the definition might be used in practice: For retailers such as Migros, shoplifting is a major threat. Detecting this security problem over time could be very valuable for Migros. After all, comparing the probability of damage occurring over time can help answer questions such as "Is the problem relevant?" or "Do we need to take measures?” A comparison between different branches simultaneously can also help identify important factors that promote shoplifting. Migros can make better decisions based on such comparisons (Bauer 2019).

Manunta (Manunta 1999) defines security as the interaction between Asset (A), Protector (P), and Threat (T) in a given situation (Si). Formally, the following function presents this definition:

$$S = f(A, P, T)\, Si$$

According to Manunta (Manunta 1999), the interplay of security activities and danger is a prerequisite for security. If one of the three core elements (A, P, or T) is missing, this will empty the concept of security of its significance. In other words, in the absence of assets, there will be nothing to protect. The contrary argument holds as well. If there is no threat, there will be no need for protection. Finally, if no protector is available, then no one will be seeking security (Manunta 1999).

The spotlight is on defining security in the context of being a condition and state for objects, people, and systems in general terms, and not on the functionality of systems. Unlike Baldwin (Baldwin 1997), Manunta (Manunta 1999) defines security not as a state but as an interaction. An interaction requires that the actors involved react to the previous actions of the others. The fulfillment of this prerequisite can happen if one considers more than a single moment. Manunta's definition of security (Manunta 1999) as interaction implies that security is not considered a snapshot but a dynamic system with different actors over time (Bauer 2019). This approach of accepting "conditional safety" for security definition is more suitable for a complex world where new threats are increasing daily, especially with increased technology dependency. This approach applies to defining "Societal Security" later to serve the purpose of this dissertation.

For quantitative safety comparisons, the definition of Manunta (Manunta 1999) is inferior to Baldwin's (Baldwin 1997). On the one hand, modeling the interactions of the core elements (A, P, and T) is very complex, but on the other hand, the reactions of the actors involved are often uncertain. Manunta's definition, however, lends itself as a basis for the development of specific strategies. Including the three core elements in a dynamic system helps the strategy developer maintain a holistic view so that one can anticipate the actors' reactions and adapt the strategy accordingly (Bauer 2019). In summary, Manunta's definition (Manunta 1999) is less useful for identifying security problems but more for designing measures. The systemic dynamic approach to security provides a solid basis for holistic problem-solving.

Smith and Brooks (Smith and Brooks 2013) criticize the theoretical definition of Manunta (Manunta 1999). Although the security function could be applied widely, it does not contribute to a better understanding of security (Smith and Brooks 2013). However, Smith and Brooks do not offer a universal definition. The concept of security is too multidimensional for a universal definition (Bauer 2019). Nevertheless, when security is a context, it becomes possible to formulate a definition (Smith and Brooks 2013). The criticism of Smith and Brooks (Smith and Brooks 2013) is encountered by the fact that a simplified, generally formulated security concept is an important working tool. It is possible to extend the general definition and adapt it to specific, more complex situations (Bauer 2019).

Exploring different definitions of security will help understand how authors and scholars from different disciplines have perceived security and will also help form a modern understanding of security in the countless branches of security applications. However, the main motive for exploring some of the existing definitions of security is to be aware of the various approaches to tackling security breaches as much as possible. The discovered definitions should help form a comprehensive understanding of what is considered security and what is not. Defining "Societal Security" will implement this approach. The definition of "Societal Security is necessary for designing Smart Sovereignty which is supposed to provide security for Society 5.0. In data protection, (Kounavis et al. 2020) proposed security models against data corruption and replay attacks. According to the model, security comprises two kinds of adversaries. Therefore, they introduced two definitions of security in this term: 1) Security is "protection against data corruption" attacks. 2) Security is "protection against content replay attacks" (Kounavis et al. 2020).

In terms of the science of security branches, Brooks (Brooks 2010) investigated the following two questions: 1) What are the categories of knowledge and subordinate concepts of security? 2) Is it possible to develop a framework of security science?

As a result, he defined 13 core categories of security; namely: Criminology, Business continuity management, Fire and life safety, Facility Management, Industrial security, Information and computing, Investigations, Physical Security, Safety, Security law, Security risk management, Security management and Security technology (Brooks 2010).

Security covers a very broad range of knowledge areas. Changes in the economy and society influence the relevance of individual areas. Undoubtedly, advancing digitization is making the

core category of information and computing increasingly important (Bauer 2019). Despite that Organizations face rising issues as a result of information security and cyber security in a world that is becoming more digital and networked (Teufel et al. 2020), Brooks omitted cyber security and information security in his list. He possibly regarded them as a form of the information and computing core category, but that will be a mistake. Consequently, it makes more sense to present them as separate independent categories of security due to their significance in today's digital revolution.

The two terms, information security, and cyber security are very close. Some authors use the terms synonymously, while others draw clear boundaries. The ISO standard (ISO 2014) defines information security as the "preservation of confidentiality, integrity, and availability of information". The three properties of Confidentiality, Integrity, and Availability are referred to as the CIA triad (Bauer 2019). Confidentiality means that only authorized persons have access. Integrity describes the correctness and completeness of information and processing methods. Availability means authorized users can access the information and associated channels when needed (Bauer 2019). The ISO standard covers information in all possible forms, both digital and analog. For example, protecting a filing cabinet with printed documents also falls under Information Security. To ensure the security of information, the protection of the associated systems that use, store or send information also falls under Information Security (von Solms and van Niekerk 2013).

Cyber security aims to protect all assets accessible through cyberspace. Cyberspace is generally understood to be the Internet (Bauer 2019). The ISO standard (ISO 2012) defines cyber security as " the protection of privacy, integrity, and accessibility of data information in the Cyberspace". Von Solms and van Niekerk (von Solms and van Niekerk 2013) complement this definition by emphasizing that cyber security protects not only electronic information but also cyberspace itself, technologies that support cyberspace, users of cyberspace, and their interests. In contrast to information security, the assets to be protected are not only composed of information but also people, their interests, and the underlying technologies (Bauer 2019).

For a modern understanding of security thinking, one needs to know that an insecure state happens when threats and risks endanger the society or the system for many reasons and in different contexts and levels of danger. When this state is absent, security can be reached or achieved. However, if the understanding of security is limited to avoiding insecurity, there will

be a shortfall in properly protecting society and the system. Therefore, it is important to note that security should not be defined and recognized as a state that can be reached only due to the absence of threats and danger, nor by hinting that it occurs in an environment with common sources of danger or attacks. That would be a negative or passive understanding of security as one should address security as carried-on activities in society. These activities and endeavors can secure the system and society (Grizold 1994). The links between security and human needs should tie in because this has been the case throughout the history of our societies, and this should not change. The principles for a modern and correct interpretation of security should derive from understanding the importance of these ties and from comprehending the unprecedented complexity of threats that our society today is increasingly facing.

For a long time, security, particularly cyber security, was framed as a tactics problem focused on how to defend the systems against threats and grant the safety of the assets. However, a greater purpose can be missed by continuing down this road. That is securing the systems' capability to generate products and services for society (Young and Leveson 2013). Just protecting the system should not be the goal of security. That should proactively assure the highest levels of security for the system and its services. Practically, according to (Young and Leveson 2013), this implies shifting security analysis from the traditional principles of just waiting for the attacks to happen (tactics), more to broad socio-technical vulnerabilities that ease the path for attackers to cause disturbances and violations of the system (strategy). To put the idea more simply, it is about the difference between reacting to the attack and being proactive in the defense mode.

2.2.1 Notions for Security in Society 5.0

This section presents some important notions and concepts related directly to security. These terms are particularly important for Society 5.0 and Industry 4.0, and they appear in many studies that address security challenges and especially for information technology, cyber security, and future society (Reveron and Savage 2020; Aldabbas and Teufel 2016; Deibert 2018; Godfray et al. 2010; Wheeler and Braun 2013; Paravantis et al. 2018; Schlienger and Teufel 2003; von Solms and van Niekerk 2013; Gcaza et al. 2017). This dissertation is concerned

with society, and all these terms matter to every society in some way or another, so they should not be overlooked completely.

In the beginning, it is suitable to talk briefly about the term safety and its use, so that it will not be confused with the term security.

2.2.1.1 Safety Concept

Frequently people confuse or mix the concept of safety with security. In some languages, there is no distinction in definitions, or the word safety does not appear separately from the word security. This section is necessary to clarify any confusion. It also adds value to the dissertation by not omitting a regularly used term and is often interchangeable with security. The distinction between safety and security has always been difficult due to the same context in which they are both used and the similar properties they carry. Since the early 1990s, there is still ambiguity in defining each and making a clear differentiation between the two terms. Burns (Burns et al. 1992) argued that there is very little distinction between safe and secure, even on a linguistic level. In German, for example, both words give the same meaning despite the technical terminology that intends to point out some differences between these terms. Many matters can be dealt with as safety or security equally. The examples of Burns (Burns et al. 1992) are a good illustration of this point; illegal adjustment to the Read-Only Memory (ROM)'s contents in a car's braking system can result in severe damage. According to (Burns et al. 1992), this example poses a problem of security, a problem of safety, or a problem between the two.

Some analysis is necessary to set boundaries that help distinguish between safety and security. The distinction is based on the nature of the harm and the relation between the actions causing the damage is reasonable. There are advantages to making this distinction. According to (Burns et al. 1992): deciding what safety is and security helps on an engineering level by facilitating the design of a system and reducing the critical components. It also helps evaluate the alternatives where safety is the main issue in focus, in addition to promoting better analysis skills.

In the 1990s, security for many refers to intentional violations while safety refers to the damage caused to a community's resources or inhabitants (Burns et al. 1992). However, these simplified concepts of safety and security do not provide a clear separation and differentiation

between the two terms. There was also a distinction between the logical and physical assets. (Burns et al. 1992) Burns explains that security was commonly coupled with logical resources like money.

Meanwhile, safety is coupled with physical assets like buildings and humans. However, this approach is still confusing, especially in situations where the interaction of machines -which carry value- and humans. This approach shows weakness in defining the nature of such an incident.

In their attempt to define safety and security, (Burns et al. 1992) started with an intuitive understanding of safety and security to derive their final definition. However, the approach they used describes the failure of the system. The nature of the failure decides if it was due to a safety or security problem. Their conclusion was the following: If the behavior of a service causes immediate harm to the resources, then it is a safety matter. If the behavior of a service causes partial harm to the resources, then it is a security matter. The work of (Burns et al. 1992) cast light on important matters and proposed a good approach to distinguishing safety from security. However, the building of the approach and the intuitive concept were better indicators of understanding a new method to differentiate the two terms than the research outcome. One of the major drawbacks of their definition is that they did not come up with definitions. They categorized the type of failure after the damage has occurred, which does not serve the system any good. Nevertheless, their work inspired a novel approach.

The notion of safety is extensive and covers many branches of science like criminology, healthcare, public security, and justice (Maurice et al. 2001). Understanding and defining safety as a concept causes much confusion for researchers. For some researchers, safety means stopping a crime from happening and preventing violence. Other researchers see safety as the feeling of keeping out of danger, and they do not consider safety a state. The varied conceptualizations do not necessarily prevent harm (Maurice et al. 2001) which makes clarifying this concept necessary to understand its many aspects.

Maurice (Maurice et al. 2001) set four basic conditions to reach an optimal level of safety. The responsibility for these conditions is not limited to the communities and the governments. Individuals should also contribute to achieving and maintaining that level of safety. These conditions are presented with minor modifications: 1) The need for an environment of social solidity, peace, and equity between parties that protect human rights and a free society. 2)

Respecting individuals' values and integrity to assure harmony and coexistence of persons with different social backgrounds and beliefs. 3) The deterrence and control of injuries and what results in physical or psychological harm. 4) The readiness to intervene in case of unwanted occasions and the existence of means for the intervention. However, the availability of all four conditions (Maurice et al. 2001) is not a natural state that demands too much from society and individuals. The absence of any of these conditions implies the absence of safety altogether, which means there is no safety in our life. Reaching an optimum level of safety is unreality whatsoever. If we assume that we have all the necessary means to prevent any harm and to intervene, do not the mean of protection need means of protecting themselves? This brings us to an endless circle of protection. Nevertheless, reaching a high level of safety is desirable, important, and satisfactory. Maurice (Maurice et al. 2001) defined safety to be an objective state: “a state in which hazards and conditions leading to physical, psychological or material harm are controlled to preserve the health and well-being of individuals and the community”. This definition seems to comply with the consensus of approximately 50 experts from various disciplines such as social services, sports, municipalities, and transport.

The safety and the safety of patients are used when speaking in the domain of healthcare. Safety in this domain is defined as “the reduction of risk of unnecessary harm to an acceptable minimum”. This definition is agreed upon by the International Patient Safety Classification (IPSC) by the World Health Organization (WHO) (Runciman et al. 2009).

Since the early 1990s, there has been a quick widespread expansion of principles and concepts for studying the relationship between management and risk. Simultaneously, risk analysis and management were applied intensively to safety matters and security challenges. These tendencies are driven by the enormous dependence on information transformation through countless communication channels and means. In the modern information society, we witness a new level of complexity of infrastructures like the 5G and interconnections of systems and organizations. All of these together result in more weak points in the systems and make them more prone to threats which motivate risk management research and push it forward (Aven 2007).

The meaning of risk is very broad and is seen from many diverse perspectives in the security setting. Risk is a mixture of consequences, related probabilities, and unpredictability (Amundrud et al. 2017). On the other hand, risk is a case where a possible threat will occur, so

the risk is defined in three pillars: assets, threat, and vulnerability. From this point of view, the risk is the interaction between threats against assets, while these assets are vulnerable to that threat (Amundrud et al. 2017).

The triangle of assets, threats, and vulnerability remain the dominant understanding of security risk in the security community. Many researchers claim that safety, connected strongly to the consequences and probability, does not apply to the concept of security. They argue that probability is rather unsuitable for labeling the risks linked to bad intentions of causing harm. The notion of judgment and the ability to harm is appropriate for risks. Then comes the following question in defining the risk: are the attackers able to strike, and do they intend to harm? (Amundrud et al. 2017).

The terms safety and security sometimes depend on the context and largely on the industry. For example, in tourism management, it is impossible to distinguish between safety and security. Security is often coupled with facilities and establishments, while safety reflects people's feelings of being protected from danger, as this appears in the work of (George 2003) and the work of (George and Booyens 2014). For instance, the work of George (George 2003) studied the perception of tourists in South Africa of safety and security but could not define what security means nor what safety means and if there is a difference between both terms. (Kővári and Zimányi 2010) addressed the issue of the importance of safety and security in the age of global tourism but still did not differentiate the two terms of safety and security.

Perhaps the reason behind this mix of these terms in tourism is that there is no tangible benefit to making such a distinction. The terms were rather coupled most of the time. When the word safety or security was mentioned separately from the other, there was no clear explanation, and no clear difference was implicit in the text is the intuitive understanding that matters in this case, especially since there are no IT systems that need to secure in the tourism industry. The focus is usually on the tourists' safety and the tourism destinations' reputations. This tendency to attribute safety to personal feelings and security within establishments does not match nor come close to the differentiation concept offered by Burns (Burns et al. 1992). It is hard to attribute this gap in the definitions to the specialty of the tourism industry because every industry is unique in its way. There might be two reasons for that:

1) The lack of research in the tourism industry about the meanings of safety and security.

2) The little difference that the distinction can contribute in general to tourism.

When we refer to a drink and say it is safe, we inherently mean that it causes no harm. We cannot refer to it as secure if our intention is the same. When we say a place is secure, we mean that it is protected from outside risk. That is the intuitive difference between safety and security. However, one can say that people are safe, and not mean that they cause no harm! The meaning here is that they are being protected from outside danger. Here lies the difficulty of distinguishing safety and security, but for us humans, it is much easier to understand the context of the talk than to precisely define what safety and security are. In the last example - people are safe- we can alternatively say: people are secure, and the meaning will remain the same. There is an interaction between safety and security, and it is hard to separate them. The same phenomenon appears in literature as well. (Eames and Moffett 1999) addressed the issue of the interaction between safety and security and argued that it is necessary to have a level of integration management for safety and security. They found in their research that if the terms safety and security requirements shall be treated separately, there is confusion and an unjustified mix between the terms, which can cause inconsistencies and disputes. That is why a level of integration is necessary to harmonize the safety and security requirements processes.

Safety definitions

Oakes (Oakes 2009) explains that the history of safety science goes back to the early twentieth century. The main emphasis of safety science was on protecting people from danger, whether due to natural reasons or caused by humans. Safety science applies to employees, workers, businesses, and goods. The science of security was created later.

The absence of safety in a society means a state of fear and exposure to danger. The opposite will be a steady state of safety. Safety then includes what adds to preserving the society's steady state, either socially or physically (Oakes 2009). No doubt, the state of safety needs endurance and constancy throughout time. Especially with the term safety can be compatible with security (Amundrud et al. 2017).

The remainder of this dissertation will use only the term security, as it is more global, dominantly used in literature, and can accommodate the term safety.

2.2.1.2 Human Security

The United Nations founded the modern concept of human security and defined it as “freedom from fear and freedom from want” (United Nations 2010). Most governments consider human security to be a soft issue that touches the lives of humans in terms of providing proper education, a well-established healthcare system, supporting people in poverty with their basic needs, creating jobs, and ensuring economic stability for the people (Reveron and Savage 2020). Therefore, human security is a human-centered approach that targets the well-being of the people and gives them their basic needs and rights. These rights and needs lay in the charters of the universal declaration of human rights (Reveron and Savage 2020).

Human security is overwhelmed with challenges and barriers such as climatic change, pandemic diseases, poverty, crimes (Reveron and Savage 2020), weak governmental systems, bad education systems, poor nutrition, and the list goes on and on. The term human security rarely pops up in developed countries because human security has very strong ties to the countries' development policies (Reveron and Savage 2020). The Covid-19 pandemic is a great example of human insecurity due to its consequences on the economy and society (Reveron and Savage 2020).

Several actors usually face human security who intend to cause damage from inside the system or the country and outside like an opposing country. The insiders pave the path for outsiders’ invasion deliberately or unwillingly by causing cracks in the human security system (Aldabbas and Teufel 2016), which weakens its response to defend against the outsiders’ attackers. Livelihoods and providing essential substances for people have always been the biggest concerns for developed countries. The cause of challenges to livelihood are countless. To name some: corruption, lack of infrastructure, poor healthcare system, limited resources, drought, poor economic performance, and other complications. According to the UN, the other face of human security is the freedom of fear habitually confronted by governmental surveillance and manipulation (Reveron and Savage 2020). Visualizing cyber security as part of human security and digital human security makes the individual in the society and the security of the systems where they work a priority for modern human rights (Deibert 2018). Most countries consider that international law is appropriate for cyber security, and their governments acknowledge the pertinence of the universal declaration of human rights (Rona and Aarons 2015). In Europe, the European Union (EU) applied the General Data Protection Regulations (GDPR) in 2018

(European Union 2018) with three key principles for processing personal data. These principles mirror the European human rights laws, which stress that individuals preserve the proprietorship of their data, deny the idea of data localization, and assure data-free movement. The three principles are: safeguarding privacy rights belonging to the individual, endorsing transparency in data processing, and assuring the free movement of data (Reveron and Savage 2020).

Human security is strongly related to the "Security of Things". More insight will follow in chapter 2.2.1.5. Nevertheless, from a human-machine perspective, security has two major categories: human aspects and technical aspects. The human side of security consists of matters related directly to the behavior of individuals. In comparison, the technical side is pure machine-related matters (Aldabbas and Teufel 2016).

2.2.1.3 Digital Human Security

The information space and cyberspace are expanding rapidly, with more content being available online day after day. This space is growing bigger than the hardware, the network systems, and the telecommunication infrastructure (Reveron and Savage 2020). In cyberspace, individuals can live within different personas on social media, web blogs (Reveron and Savage 2020), game platforms, streaming sit, and other forums. Often people see cyberspace as a new dimension where people will encounter novel challenges to reality (Reveron and Savage 2020). The virtual world will become an extension of the real world (Johnson 2008), and we might end up living in both worlds differently at a time.

(Johnson 2008) explains that the virtual worlds have become so essential for our real world that they bring together people from different nations, cultures, and languages in several ways crossing all the natural, cultural, and political barriers. The richness of the quality of modern communication can be to a certain level compared to face-to-face communication. These new means of communication enable teams to work together remotely and efficiently worldwide, develop software, run businesses, share experiences, and build solid relationships. Cyberspaces push toward redefining education, teleworking, and shopping.

Undoubtedly, there are new horizons for research and developments to discover, and new possibilities that never existed before appear because the geographic and political barriers are disappearing. In the era of the Covid-19 pandemic, the importance of these cyberspaces is

getting significantly higher to an unprecedented level which is easy to spot with the increased market values for big tech companies like Amazon, Microsoft, Apple, Tesla, and the list goes on (Braithwaite 2020).

Modern communication methods could never have reached their current level of efficiency if it were not for the global fiber optic networks that made the connection between people all over the world very practical. The future of the internet connection might be the space internet which will help better connect disconnected countries. Supply chains and access to a wide variety of data enjoyed their share of advancement and technology boosts (Reveron and Savage 2020). Estimations suggest that over half of the world's population uses the internet daily (MM Group 2011). More recent estimations indicate that over 57% of the population around the world used the internet regularly in 2019 (World Bank 2019). Within the last ten years, people worldwide have become reliant on the digital world in their daily routines as much as they are reliant on the real physical world (Reveron and Savage 2020). The cyber connections between nations worldwide, within, and across cultures have enormous effects on economic expansion and advancement, especially for poor regions. These connections allow countries to conquer the challenges of being isolated from more advanced countries like the U.S and western Europe (Reveron and Savage 2020).

Digital human security is intertwining deeply and more intensively with human security. The bounds tie harder with time, and soon -if not already- the separation of digital security and human security will be difficult. Modern means of communication spread internationally and have become very common. They carry huge loads of knowledge that we can use relatively easily. Reveron and Savage (Reveron and Savage 2020) make clear that strong computational techniques and AI have big potential to improve our lives and are in use already. An example of the strong effects of these technologies is visible during the Covid-19 pandemic when countless workers shifted to work from home during a partial or complete lockdown, not omitting schools and universities opting for online education. People continued to connect in almost perfect conditions despite the challenges.

One should not get too carried away with all the positive impacts of modern technologies on our lives, education, work environments, and businesses. Each advanced technology carries some vulnerability that weakens digital and cyber security and demands more protection to preserve human security. With every adapted technology that changes a daily routine comes

a cyber threat that threatens this routine. That brings us to stress that new technologies are challenged with unprecedented risks and require more investments in their security. For instance, once the entire society depends on e-payments to pay their bills and purchases, a small breach in the e-payment system, or a power shortage will paralyze all payment activities and disrupt the retail industry. In this case, one cannot go back in time and pay only with cash to prevent such disruption. That is no longer efficient and will most likely not be acceptable by society as a solution. What can solve the problem is a rather more efficient and secure payment system.

Without proper cyber security guidelines and frameworks, cyber-attacks will only generate fear and uncertainty in information technology and almost every industry, hindering society's advancements and productivity. Therefore, digital security should and is indeed a universal concern for governments.

Humanity is opposing a vital challenge: to master the technologies of cyberspaces and manage the abuse of these technologies so that the full capability can be reached (Reveron and Savage 2020). Governments must be very active in digital security to convene stakeholders and set regulations for information technology services just like they regulate other products and services. The main aim is to protect the market from manufacturers who intentionally and unintentionally underestimate the end user's security. Information security guru Schneier explains how the digital marketplace will require regulations (Hall 2017). Hall argues that technologies, in general, come with three attributes that one can select only two of them: good, fast, and cheap. Most corporations, if not all, select fast and cheap and leave the attribute “good” behind for the user to struggle. Big corporations like Google and Apple have an army of engineers whose job is to fix the bugs that appear in the system. We see that through the regular updates for the software operated by these corporations. However, other small companies do not provide such services, leaving loopholes in the systems that practically breach, making them vulnerable. Therefore, according to Schneier, governments must intervene and regulate these digital products to prevent such practices as companies will not voluntarily provide these services.

Here, one has to distinguish the difficulties of a secure cyberspace method, which differs greatly from traditional protection methods. In general, within a country, several players cause difficulties for the government's sovereignty. These players hinder the power to reach security.

This affects securing spaces for people on land, in the air, in the sea, or even in cyberspace. The case of cyberspace is a different story as the governments are either passive in terms of the latest protection means or follow what big companies dictate. However, often rather than less, ICT companies are driven by business and notational security goals (Reveron and Savage 2020).

Governmental reactions to cyber threats and attacks do not meet the challenge at hand, which causes a gap between the risks and the responses. The periodical reports of cyber breaches indicate the existence of such a gap. The biggest threat to individuals appears to be related to cyberspaces (Reveron and Savage 2020).

2.2.1.4 Future of Cyberspaces

Since the early 1970s, governments have been advancing in understanding the importance of IT (information technology) by exploiting the experiences of the private sector. The first version of the internet where people are anonymous and no borders exist between users when connecting is from the past. In Europe, efforts are to broaden human rights in cyberspaces and consider them equal to physical spaces. However, somewhere else, far away in the east, China is leading the undermining of human rights and cyberspaces. A form of digital repression is easily seeable (Reveron and Savage 2020). This new phenomenon of the EU increasing human rights security and China suppressing it is nothing but a reflection of certain limits and the significant differences in the political system and the political culture between the two regions (Reveron and Savage 2020).

Countries worldwide are developing and investing in their cyber control to protect their sovereignty on their territory at the very least. Cyber security matters are growing in terms of their influence on national security. Therefore, the focus of governments concerning rivalry has to shift accordingly, which implies that they have to shift from traditional war thinking to a digital approach of seeing the future of security and understanding how modern competition will affect the people, the businesses, and the cyberspaces (Reveron and Savage 2020).

Information and communications technology have a promising potential to improve economic development and lead to social advancement. However, at the same time, like any other tool invented by humans, it carries the potential to increase misery and divide society if exploited with ill intentions (Reveron and Savage 2020). Today, the internet has become a domain for

crime, spying, blackmailing, and the international security environment is getting closer to becoming Pandemonium (Geers 2010). Only efforts in setting national regulations and international laws and forcing ethics in technology can reduce the effects of the chaos caused by cyber-crimes, especially since the internet has become simultaneously a commercial space, social space, and even sovereign space (Reveron and Savage 2020).

Despite the advancements in security software and security measures and their advanced programming skills and AI, the security of cyberspaces will be more complex because the hackers are equipped with good programming and strong encryption, not forgetting AI that they can use. In simple words, the game moves to the next level. Reveron and Savage (Reveron and Savage 2020) stress that there is no easy answer to these difficulties, and human behavior here will play a vital role, and one must take it seriously to improve digital human security. The participation of all individuals is needed to enhance the security of cyberspaces. However, the last recommendation did not come with any further explanation or indication of what approach the behavior of digital/cyberspace users should apply and in what direction exactly. Above all, what are the possible paths to go in digital spaces? The answer to this question is a very interesting and fertile field for research.

There is no doubt that the future of cyberspace and its security is, to a certain limit, ambiguous with much uncertainty. The mystery lies in discovering how technology will change, how this change should integrate, and how it will impact society on its variance of levels like social, political, economic, and national security. Figure 2-5 illustrates this thought.

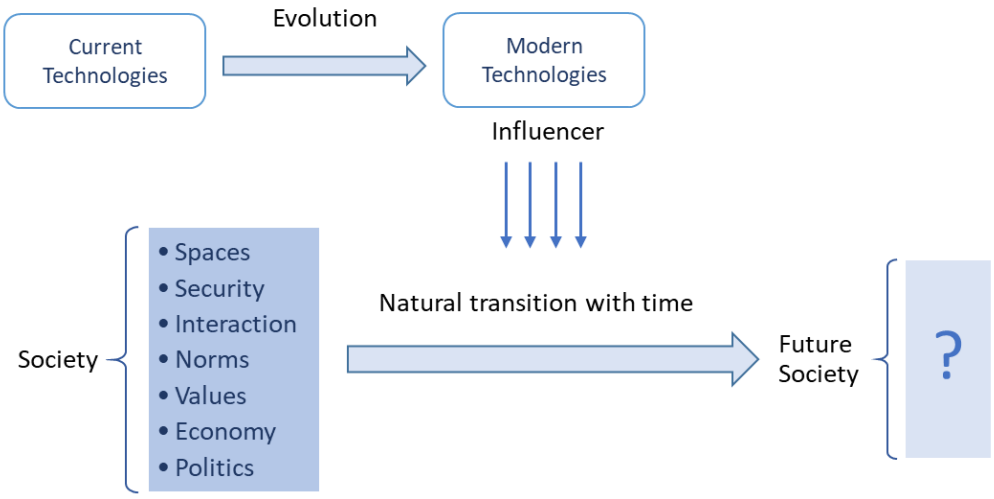


Figure 2-5: Mystery of Future Transition

Using the internet is not a luxury as it was in the 1990s. It became a digital necessity to remain connected and active in society. Governments are aware of this obvious fact and strive to make cyberspaces safe for users by supporting digital human security (Reveron and Savage 2020). Nevertheless, the mission is extremely difficult and requires the participation of responsible digital humans.

2.2.1.5 Security of Things, and Human Security

Human security comes at the center of attention when discussing any security matter. The security of things, therefore, is strongly coupled with human security.

Safeguarding human security means securing everything around it, including food, energy, information, cyberspaces, data, and other security matters. Figure 2-6 shows security things that need to be secured to achieve human security.

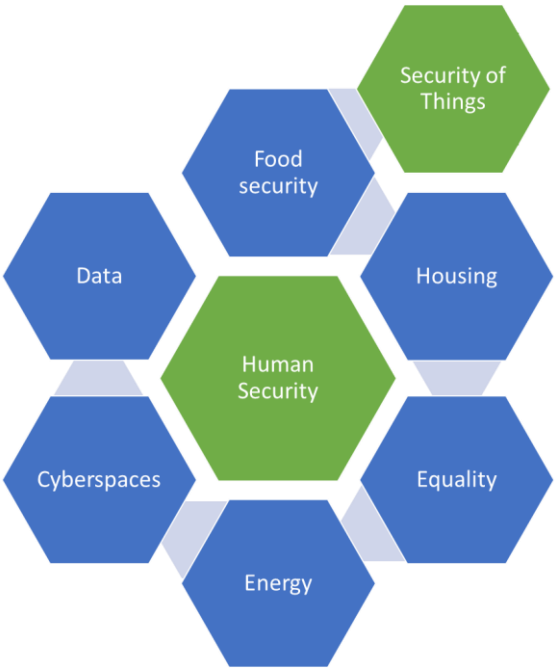


Figure 2-6: Security of Things and Human Security

All elements connect to the "Security of Things"; once this chain is complete, human security will be achieved too. As explained the Figure 2-6 the components of human security are the basic security needs in the current society. Human security forms the bottom two layers in Maslow's pyramid Figure 2-4 put in the context of current society. The following section elaborates more on these security elements.

2.2.1.5.1 Food and Housing Security

The concept of food security, or food and nutrition security as sometimes referred to, emerged dramatically in the past few decades theoretically and practically. The common wildly accepted definition for this concept was “secure, adequate, and suitable supply of food for everyone” (Gross et al. 2000). Food security concerns go back to the early forties of the last century. Food security will continue to be a global concern for at least the next 50 years. Not only food shortage and climate change but also water scarcity are part of the problem for food security (Rosegrant and Cline 2003). One should not ignore the increasing population; growing food consumption has led to bigger global demand for food for another 40 years (Godfray et al. 2010).

The definition of food security evolved considerably over time (Gross et al. 2000). According to the Food and Agriculture Organization (FAO), food security is ‘‘situation that exists when all people, at all times, have physical, social, and economic access to sufficient, safe, and nutritious food that meets their dietary needs and food preferences for an active and healthy life’’ (FAO 2001). Gross (Gross et al. 2000) defines food and nutrition security as follows “Food security is achieved if adequate food (quantity, quality, safety, socio-cultural acceptability) is available and accessible for and satisfactorily utilized by all individuals at all times to live a healthy and happy life”.

The two mentioned definitions above include accessibility and availability of food. These two terms appear over and over in most definitions of any security-related term. Figure 2-7 presents the food security framework of Gross (Gross et al. 2000).

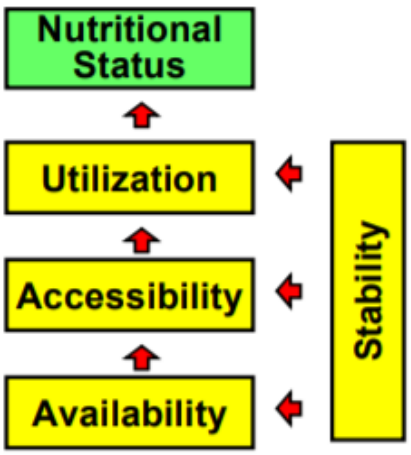


Figure 2-7: Food Security and Nutrition (Gross et al. 2000)

Climate change creates a serious risk of hindering the endeavors toward a world free from hunger as it impacts crop productivity and has potentially severe consequences on the availability of nutrition (Wheeler and Braun 2013).

There are four essential elements for food security: namely availability, stability, utilization, and access. However, simulation studies address only availability (Schmidhuber and Tubiello 2007). Climate change endangers all four elements of food security and food availability. The effects of climate change on food security vary depending on the country's region, time, and socio-economic situation. Assessments and simulations show that developed countries will be severely affected and have to increase their import dependency (Schmidhuber and Tubiello 2007). Besides climate change, other food challenges security the increasing competition over land, water, fisheries, and energy, reducing the ability to produce food (Godfray et al. 2010). Ending poverty and hunger are two of the UN's Sustainable Development Goals (United Nations 2020), and meeting the food security challenges is vital to reaching these two goals (Rosegrant and Cline 2003).

Housing security, equality, and non-discrimination are no less important than food security, as the United Nations assures (OHCHR 2022). Some of the most important characteristics of secure housing are availability, affordability, cultural adequacy, and habitability. However, discussing every aspect of human rights is out of this dissertation's scope. It is enough to reference some and discuss some if they serve the main intention and aim of the research.

2.2.1.5.2 Energy Security

Energy security emerged as an important matter with the oil crisis that hit the west in 1973 and exposed the fragility of developed economies to oil price shocks. The political clashes between energy-producing countries pushed energy security to become the main concern for countries worldwide(M. Kékes and L. Gábor 2015). Since then, countries have started seeing energy security as a part of their national security (Paravantis et al. 2018).

The International Energy Agency defines energy security around two keywords: availability and affordability. They define energy security as "the uninterrupted availability of energy sources at an affordable price" (M. Kékes and L. Gábor 2015). From a completely opposing perspective, some specialists took a different approach and defined the concept of energy security by stressing the absence of energy as a core for their definition (M. Kékes and L. Gábor 2015).

They define energy security: “energy insecurity can be defined as the loss of welfare that may occur as a result of a change in the price or availability of energy” (Bohi et al. 1996).

The prosperity and sustainability of any country require that this country has energy security that is also periodically evaluated. However, researchers did not yet reach an acceptable definition of energy security (Nelwan et al. 2017). (Ang et al. 2014) state that energy security has been a broad domain for research, especially in the past decade, and is a serious matter for numerous stakeholders such as policymakers, a variety of industries, and communities (Ang et al. 2014). The definition of energy security focuses on the availability and supply of energy (Moran and Russell 2008) and pricing (Spanjer 2007). However, other researchers say that a comprehensive definition of energy security should include other downstream effects like the influence of energy security on the economy and the welfare of society (Vivoda 2010). It is difficult to uncouple the general concept of energy security away from matters like oil disruption, gas, and electricity. As a result, energy security has already become a political subject worldwide (Paravantis et al. 2018). The significance of energy security is increasing in Geopolitics for several reasons, like increasing energy prices worldwide with international demand, the fear of supply shortage because of the scarcity of resources, and the apprehensions of social and political impacts due to climate change (Vivoda 2010). Scarcity of resources can also be intentionally created for political and war strategy reasons like when Russia shut off gas shipments to numerous EU countries following the invasion of Ukraine in 2022 (Zhou et al. 2022).

Security’s traditional approach is dominating the foundations of energy security, which implies a different understanding of energy security in different geographic locations as well as of different historical experiences (Paravantis et al. 2018) for the nations, their political system, and their economy (Luft and Korin 2009). This approach is apparent in the policy of Western European countries and their weak dependence on importing gas from Russia. (Leonard et al. 2007) attribute the origin of this breakable dependence to the Cold War, resulting in variations in energy security concepts.

The definition of energy security is highly dependent not only on the context in use (Ang et al. 2014) and on the country-related situations in terms of geographic location, natural resources, political relationships, economic development, and ideology (Paravantis et al. 2018).

Unsurprisingly, like the definition of security itself, there is no consensus on the definition of energy security. Energy security is dynamic and highly contextual (Ang et al. 2014). By the year 2014, there have been 83 variants of definitions for energy security (Nelwan et al. 2017). After implicit and explicit analysis of several energy security definitions, (Chester 2010) concluded that the energy security concept is slippery because it has a polysemic nature. (Ang et al. 2014) Moreover, Nelwan (Nelwan et al. 2017) urges that the definition of energy security should be revisited periodically to ensure it stays relevant to the matter and up to date.

Seven energy security domains have been identified by (Ang et al. 2014) and are based on 83 different definitions and studies: availability, infrastructure, prices, societal effects, environment, governance, and efficiency. These are the same seven dimensions Nelwan identified and referred to as the 7D concept (Nelwan et al. 2017). On the other hand, (Paravantis et al. 2018) took a different approach to defining the domains of energy security. In the adapted geographical perspective to look at and analyze energy security, the dimensions comprise environment, technology, demand, sociocultural and political factors, human security, geopolitical contemplations, and energy security policy (Paravantis et al. 2018). However, there is still some acceptable level of correspondence with the 7D concept, but not without emphasizing the roles of the geopolitical environment.

The matter of measuring energy security is even more complex than defining energy security itself. The reasons behind this difficulty are simply the different historical and geographical circumstances of the environment where energy security is defined (Paravantis et al. 2018)

The World Energy Council, World Energy Forum, and US Chamber of Commerce have published their concepts for energy security. The three different approaches by these institutions result in variations of explanations for energy security (Narula and Reddy 2015). Nevertheless, all of their definitions and concepts include all the domains of security, namely the 7D (Nelwan et al. 2017).

The new slogan in the recent literature suggests that the solution for energy security is “going green”, which regularly accompanies sustainability (Choong et al. 2014). Sustainability refers primarily to improving and deploying clean energy and pursuing economies and lifestyles with low energy consumption and efficient energy use (Choong et al. 2014).

Instinctively, the expectations to improve and sustain energy security would be by increasing renewable energy resources like solar energy, hydro energy, and wind power onshore and offshore. These can contribute by reducing the dependence on traditional energy sources (Choong et al. 2014). Likewise, changing energy consumption patterns (Aldabbas et al. 2015) contribute to energy conservation and efficiency, eventually reducing energy demand growth(Choong et al. 2014). Furthermore, improving technology in oil-dependent industries, like the automobile industry, can impact by reducing the carbon footprint and shaping the future of mobility.

Energy literature before 2000 did not consider environmental issues to be part of the definition of energy security. Energy supply is secure if it is adequate, affordable, and reliable (Gill et al. 2015). The commonly accepted definition by the UN was “availability of energy at all times in various forms, in sufficient quantities, at affordable prices” (Goldemberg 2000). Once more, the focus in defining security terms is the common keyword availability, precisely the availability of energy resources. From 2000 onwards, a new emphasis entered the domain of energy security, which is a sustainable environment (European Commission 2001).

Availability of energy means having a secure supply, which is the main challenge confronting the economies of both developed and developing countries. The reasons for that are countless. For instance, the infrastructure systems' incapability and increasing demand for energy. Threats of cyber and physical attacks on power plants and electricity grids in addition to sometimes global oil crisis (Gill et al. 2015).

Researchers in energy security altered their definitions of energy security to comprise environmentally connected terminologies, with growing caution towards the environment. The new keywords in these definitions contain sustainability goals, environmental sustainability, and development sustainability (Choong et al. 2014). Environmental sustainability became essential for energy security literature as many researchers adopt environmental sustainability in the dimensions of energy security. The suggested path of “going green” can help to improve energy security. However, even though renewable energy contributes to the security of the energy supply and provides good alternatives for electricity generation, they are not risk-free. The costs can be, in some cases, relatively high in comparison to traditional energy supplies (Gill et al. 2015). The total costs for that are not easy to calculate. Many issues, such as economic competitiveness, stand in the face of the

shift(Choong et al. 2014). Governments should approve and undertake more efficient energy production technologies and push toward demand reduction if they want to reach greater energy security (Gill et al. 2015).

2.2.1.5.3 Information Security

One of the greatest assets of any organization is its information. Information security management largely ignores the human factor as the emphasis is mostly on technology and production. The system user is viewed as a security threat rather than a security asset. A mindset changes from a technological to a socio-cultural approach, from the notion of "the user is my enemy" to "the user is my security asset," is required (Schlienger and Teufel 2002). Implementing a new approach to culture and integrating it into the system will improve the general security of the organization (Schlienger and Teufel 2002) and, consequently, society. Surely several management concepts and techniques are required to implement the new sociocultural procedures effectively and efficiently (Schlienger and Teufel 2003).

Guarding information for organizations is getting ever more critical (AlHogail and Mirza) for countless reasons, such as securing the organization's stability, keeping its clients' trust, and so on. Failing to protect the information will be severely costly for the organization not only in terms of money and assets loss but also in destroying the organization's reputation, losing the trust of the customers and the confidence of the shareholders.

The information security concept is difficult to define because it is variable, uninformative (Collard et al. 2017), and the fact that it is context dependent as well. Most definitions are out of date and need reconsideration. Information security is becoming linked to cyber security and is often confused. The distinction of each concept is necessary.

Information security aims to secure the endurance of businesses and reduce the harm that security breaches can cause (von Solms 1998). The international standard (ISO 2014) defines information security as the “preservation of confidentiality, integrity, and availability of information”. This information comes in different forms. It could document whether it is in a printed form or stored online. It can be viewed in films, discussions, and meetings (von Solms and van Niekerk 2013). The definition offered by (Whitman and Mattord 2009) is concerned with protecting information and related assets. (Whitman and Mattord 2009) defined information security as “the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information” (von Solms and van

Niekerk 2013). Several characteristics of information security are identified by the authors mentioned above. They contain confidentiality, integrity, and availability (von Solms and van Niekerk 2013).

Evaluating information security is important for the safety of the information system. The ever-developing technologies, particularly the information industry on the internet, require higher levels of security to match the threats that wait for loopholes to create damage. The main purpose of information security assessment is to correct the errors that result from the decision-makers and keep the safety of the organizational information under control (Cai et al. 2015).

Information protection is not limited to the protection of stored information, whether stored physically on shelves or servers. The protection should also cover the wirelessly transferred data through communication systems. Modern communications systems perform the role of exchanging channels for every kind of information and data like commercial, medical, industrial, and every other possible type of data. Any attack or breach of this wireless information system can cause severe damage to the assets of the organization. Wireless communication faces challenges with its characteristics, as (Cai et al. 2015) argue. There are issues related to its need for low bandwidth and data rate, in addition to the need for low energy consumption, which is the case for small portable devices. The communication system's security requires four categories application security, device security, technology security, and server security (Cai et al. 2015). Therefore, information security is a broad dynamic field regarding what it includes and needs protection. This example can be treated as part of cyber security equally, which indicates, as will be discussed later, that cyber security is an attribute of information security. Nevertheless, it is similarly important and needs separate reconsideration.

Information security indicates the usage of physical and logical data access control to safeguard the appropriate use of data and to forbid illegal or accidental alteration of data, in addition to preventing data demolition, exposure, loss, recording, or any misuse of information assets (Peltier 2005).

(Laudon and Laudon 2010) defined information security as “the prevention of unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction of information and information systems” (Amankwa et al.). Meanwhile, International

Organization for Standardization ISO defines information security as the “Preservation of confidentiality, integrity, and availability of information” (ISO 2008).

Several authors defined information security with three keywords: confidentiality, integrity, and availability (Amankwa et al.). Therefore, it is safe to come to the assumption that the traditional meaning and definition of information security for most researchers revolves around three main things: confidentiality, integrity, and availability (Anderson 2003). The same thing applies to the definition of computer security (Bishop 2003).

Anderson (Anderson 2003) argues that all the old-school definitions suffer at least from one mutual problem: the breadth of the definition and a level of ambiguity in providing a clear meaning of what information security is. Anderson suggested a new definition for enterprise information security: “A well-informed sense of assurance that information risks and controls are in balance”. He argues that this definition does not conflict with the old-school perspective. It rather solves some inherent problems in the old definitions.

Amankwa (Amankwa et al.) said that education, training, and awareness are very valuable to an organization's information security. Once the employees are educated and aware of the threats around the security of information, they can be more responsible for guarding the organization's information security. Employees should be cautious when working with information and making decisions that can influence the safety of this information. Employees as humans are seen as a point of weakness (Aldabbas and Teufel 2016) in the information security network (Amankwa et al.). In contrast, they should be part of the solution (Aldabbas and Teufel 2016).

Several studies indicate that employees' attitudes and lack of security awareness are among the main contributors to security breaches (AlHogail and Mirza) and system weaknesses. Price Waterhouse Coopers stated in a study published in 2013 that human mistakes are the cause of most security cracks and not the technology (AlHogail and Mirza). However, this should not underestimate the importance of technology development in coping with the latest threats. The chain is as weak as its weakest episode.

Unfortunately, despite the importance of the information security triangle -information security education, training, and awareness- their definitions in the literature do not provide a tangible value or contribution to a foundation for research. The three concepts of the

information security triangle are often used interchangeably and are confused despite having different meanings (Amankwa et al.).

Finally, it is useful to hint that in each of the security-related terms like energy security, information security, cyber security, and other important matters, there are definitions for deeper terms related to the original term. For example, there are definitions for information flow security and information security culture. The same thing applies to the rest of the security domains.

2.2.1.5.4 Cyber Security

The importance of cyber security is widely recognized as many organizations face great challenges to secure their assets and maintain their cyber security (Teufel et al. 2020), but there is less agreement on how to achieve it or approach it. Additionally, the definition of cyber security is intensively researched, with over 400 definitions available on the Global Cyber Definitions Database (GCDD) alone (Deibert 2018).

There have always been debates about the definitions and the interpretation of cyber security and cyberspace safety. Some authors called it the independence of cyberspace (Maurer 2014). On the west coast of the United States, it was referred to as cyber security, while on the eastern coast, cybersecurity (all in one word). IT experts used the term information security until 1996 when the term cyber replaced the current one and became dominant (Maurer 2014). IT experts were involved with cyber security matters, politicians, and law enforcement officers. Hence, the notion of information security is different and still in use, increasing the difficulty of reaching a consensus on the definition of cyber security.

Often by many researchers, the terminology of cyber security is mixed with the term information security. However, this mix is not necessarily correct most of the time as these two separate concepts carry different meanings despite the overlap in some aspects and dimensions(von Solms and van Niekerk 2013). Both terms are not completely equivalent as cyber security extends beyond the traditional concept of information security. Like information security, it comprises securing and defending information assets and spreads to protect other assets, including the user himself. Nevertheless, only a small proportion of researchers distinguish between the definition of information security and cyber security (von Solms and van Niekerk 2013). The leading cyber security and anti-virus Lab Kaspersky define cyber security as “the practice of defending computers, servers, mobile devices, electronic systems,

networks, and data from malicious attacks" (Kaspersky 2020). It is noticeable in this definition that cyber security - as (von Solms and van Niekerk 2013) have argued – protects not the information but also the assets. Merriam Webster's definition of cyber security corresponds to the core indicators of the definition of Kaspersky. The definition indicates that cyber security is "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" (Merriam Webster 2020a). There is less divergence in the definitions of cyber security among experts and researchers than there is for the definition of security in general or the definition of energy security.

The mix between information security and cyber security might not sound like a serious issue, especially in an informal context. However, when the field of adaptation is the strategy for organizations, setting the objectives of corporations or reaching international agreements, the confusion between the two (information security and cyber security) can result in serious problems (Schatz et al. 2017).

This question is hard to answer, but cybersecurity is seen as a subset of information security from the industry's point of view. In some cases, and from the industry perspective, there is no conformation in the distinction between information security and cyber security. According to (Schatz et al. 2017), Gartner Inc. professionals (Walls et al. 2013) consider information security as a sub-category of cyber security, exactly contrary to Barzilay (Barzilay 2013), who sees cyber security as a sub-discipline of information security. However, in their guidelines, ISACA adapts a different cyber security approach. They state that cyber security is evolving within the domains of information security and traditional security (Schatz et al. 2017). Herewith, we have a trilemma with difficult choices to select only one that truly represents cyber security.

Academically speaking, (Luiijf et al. 2013) analyzed the definitions of cyber security in the shadow of National Cyber Security Strategies and found that the term cyber security is largely in use, and the definitions are highly variable, context-dependent, usually subjective, and vague (Craigen et al. 2014; Schatz et al. 2017).

The term cyber security gained much momentum after a speech by Obama in 2009 when he called on the people of the United States to recognize the importance of cyber security. That impacted the terminology significantly. Consequently, there was a steady decline in terms like computer security and information security (Schatz et al. 2017). There is a small issue with little significance: inconsistency within the literature on cybersecurity and cyber security (Schatz et

al. 2017). For consistency throughout this dissertation, cyber security (two separate words) will be used.

In recent years, security branches have expanded as technology advances. Electricity grids and power plants need optimal safety more than ever. Any weakness or breach in the system can result in fatal damage and limitation of services in different ways (Aldabbas and Teufel 2016). The protection of the premises of the power plants is no longer enough. The plants and the grids need to be secure against cyber-attacks. The level required here is beyond the capacity of security firms. Governments should take responsibility to protect their assets. Massive attacks conducted by countries against each other are common nowadays, and there are countless examples of such attacks. The United States condemned the destruction of the Georgian electricity grid in 2008 by Russia, for instance (Osce 2020).

The safety of modern energy plants and the stability of electricity grids, wind farms, photovoltaic power stations, and other new energy generators depend significantly on improving and developing cyber security defense systems (Liu et al. 2019). Power generators and the controlling grids are often easily targeted for attack by intruding on the communication between the energy generators and the controlling station, such as the grid. This communication goes through optical fiber, line communication, wireless, and networks. Here lies the huge threat of cyber-attacks (Liu et al. 2019). In the example of a wind turbine, the attacker can direct hateful signals to the controlling grid, manipulate the data, and disturb electricity production. Other security risks to power plants can be unauthorized access to the network, hijacking the wireless communication, spying, disturbance of communication, and denying the power grid service(Liu et al. 2019).

The securing technologies applied for smart and traditional grids are insufficient to guarantee a hundred percent security level. (Aldabbas and Teufel 2016) stated that humans can be the loophole for cyber attackers to enter the grid and create damage. Von Solms (von Solms and van Niekerk 2013) speaks of the role of humans and the weakness they bring to the system in both information security and cyber security. The additional role of humans as a factor in cyber security is being one of the weak targets for attackers.

Big challenges remain strongly connected to the organization, economy, and social and political systems. Not omitting that human security is indissolubly connected to cyber security

efforts. Moreover, (Craigen et al. 2014) add that the solutions for cyber security problems alone cannot be the answer for all the security weaknesses.

(Craigen et al. 2014) go further and argue that cyber security has an interdisciplinary nature after investigating many definitions and areas of application of cyber security. A former Director at the National Security Agency in the United States explains the multidiscipline of cyber security by stating that cyber security brings opportunities for advances built on a multidisciplinary. The reason is that cyber security is basically about confrontational clashes. Humans have to protect machines from attackers who use machines that require knowledge in several fields like computer science, electrical engineering, and mathematics (Craigen et al. 2014). The work of (Craigen et al. 2014) included a literature review in a broad range of disciplines with a focus on engineering, technology, computer science, and security and defense. Other disciplines were also investigated but with less attention. They found that some definitions contained non-technical terms but rather human connections. However, the majority included the technical side, which proved to be dominant in the definitions of cyber security.

Consequently, (Craigen et al. 2014) defined cyber security as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". This definition integrated most keywords derived from the literature overview considering the interdisciplinary nature of cyber security. A recent definition of cyber security by Freedom Online Coalition Working Group (the group is founded and supported by 32 national governments) suggests that cyber security is: "the preservation – through the law, policy, technology, and education – of the availability, confidentiality, and integrity of information and its underlying infrastructure to enhance the security of persons both online and offline" (Freedom Online Coalition Working Group 2015). The most important piece for the group is that cyber security must protect and promote human rights. Human rights were not mentioned in the definition of cyber security but were indicated in the preamble for the definition.

Cyber security as national security matter / human-centric cyber security

Countries that compete politically and economically for survival and to maintain their advantageous position realize the significance of cyber security and the threats that cyber-attacks can cause. They perceive these threats as threatening to their sovereignty because the

damage can reach most modern and smart infrastructures (Deibert 2018). Therefore, cyber security is a matter of national security system. Whether the state adapts authoritarian or liberal approaches, the importance of cyber security is the same, and the priority is national security (Glasius 2018). However, many states exploit the need to secure their cyberspaces to justify massive internet censorship with large surveillance and control of their citizens (Deibert 2018). Such practices are apparent in countries like China and Russia, where cyber espionage and the limit of cyber freedom are dominant in these states and strongly backed up by the ruling regimes. Achieving national security does not justify these practices, which arguably violate some human rights.

An alternative human-centric approach is necessary to replace the current practices. This approach should put humans as the primary objective of security (Deibert 2018) rather than putting control over the borders and the network systems in the center. One should not assume that the sovereignty of territory and the control over network systems are not essential for national security. That is true and very important for the security of the country. Nevertheless, the human-centric approach sees the networks as a core element for modern practices (Deibert 2018) of cyber human rights, like access to information and freedom of cyber expression. There have been attempts to provide examples and guidelines for online human rights by the Freedom Online Coalition Working Group, a group supported by 32 national governments committed to protecting and promoting online freedoms domestically and abroad. The list of countries includes Switzerland, Germany, and the United States. The major recommendations assure cyber security policymakers should protect and respect human rights. The design of cyber security development laws should focus on human rights, enhance individuals' security online and offline, and be consistent with international laws. The law concerning cyber security should not hinder any technology that promotes human rights protection. The group also stressed the importance of education and digital literacy in fulfilling human rights.

Stakeholders must work together to confront the increasing complexity and numbers of cyber-attacks and cyber-crimes in an approach that protects human rights (Freedom Online Coalition Working Group 2015). Additionally, the involvement of all stakeholders means that all individuals are also responsible for playing their role in participating in and protecting

cyberspaces. In other words, this is a social responsibility for everyone and not only a task for policymakers and governments.

Towards human-centric cyber security

There have been questions raised by lawyers concerning the application of international humanitarian laws in cyberspaces because of the importance and significance of cyber-attacks on the networks, and even a question if the term armed conflict should include cyberspace conflicts. The International Humanitarian Law has foreseen improving warfare tools and technologies since the second world war. Therefore, International Humanitarian laws inherently include cyber warfare, especially since civilians are often a target of attackers (ICRC 2010). Nevertheless, this matter remains legally not so easy to resolve. On the one hand, the attackers can target production lines, banks, healthcare systems, and every possible asset in society.

On the other hand, these attacks are not considered armed militias or violence. However, this should not leave it out of the remits of International Laws (ICRC 2010). There is an urge for International Humanitarian Laws to reformulate to regulate cyber warfare practices and list the methods of attacks as weapons, especially since the International Humanitarian Laws intend to protect the livelihood of the individuals. Cyber-attacks are a direct threat to these livelihoods. New laws and regulations that protect the dignity and livelihood of individuals in cyberspace are the core of human-centric cyber security (Deibert 2018). Without the enforcement of revised international laws which treat the cyber threat as it should be, there will remain a loophole that hinders the security of society. Already some efforts toward this achievement are in place. The Freedom Online Coalition Working Group confirms that international laws must be applied online (Freedom Online Coalition Working Group 2015). There is also broad recognition that international humanitarian laws must consider cyber-crimes as armed conflicts in cyberspace (Deibert 2018), which implies the need to reduce and limit the cyber weapons in addition to the destination between the cyber-attack targets to separate individuals from other targets. The human-centric approach to cyber security can be consistent with these revised regulations (Deibert 2018).

The current international laws that regulate sovereign states and their relationships benefit the sovereignty of the states and not the individuals (Deibert 2018). For cyber security to be human-centric, this view should slightly change, at least, i.e., the international laws should

benefit the individuals and their best interests. According to Besson (Besson 2011), international laws must prioritize the benefit of the individuals, and the states should be responsible for this entitlement.

Countries show different behavior when dealing with cyber security. In cyberspace, human rights need more protection than in the physical world as both countries and companies steadily violate human rights online, which will not change soon (Deibert 2018). The United States, China, Russia, and many other states have formal regulations and principles for cyberspaces, but all of these countries violate the practice of cyber security (Deibert 2018) either by espionage or by planned attacks. This violation results in conflict between the traditional cyber security approach which favors the states and the human-centric approach which favors the individuals. The states see themselves as sovereigns in human-centric cyber security when they should rather be the guardians and officials of the sovereignty of the individuals.

2.2.1.5.5 Data Security

Data security addresses the protection of the data and the prevention of any unauthorized access or distribution of the data (Summers and Koehne 2004), while information security has broader and wider practices that include information flow, communication channels, and information storage as having been discussed before. Therefore, data security is a subcategory of information security.

In the past ten years, data security has become increasingly used to protect the information that organizations store, process, and analyze. The reason behind this rise is the mounting number of information resources that organizations depend on (Tankard 2012). Science focuses magazine of the BBC estimates that huge online companies like Google, Facebook, Amazon, and Microsoft store at least 1.2 million terabytes of information. This figure excludes other online storing services like Dropbox (Mitchell 2020). Approximately 1.8 zettabytes of data were created and simulated in 2011 alone. This amount of data keeps growing and doubles every two years (Tankard 2012).

One of the biggest concerns for big data security regarding data collection and analysis is that companies gather and process huge amounts of sensitive data concerning clients and employees. They also gather intellectual property and other information requiring absolute secrecy (Tankard 2012). If such secret and sensitive information get exposed, the damage to

the organizations and the clients will be painful. On the other hand, companies seek to earn value by collecting a wide range of information for their customers to serve their preferences better. That is achievable by centralizing data which makes it under attack and in a risky position against hackers. It will not be limited

With the increased dependency on IoT, AI, industrial IoT, smart grids, smart meters, cloud computing, and this sort of technology, data security enjoys a bigger significant role because of all these new technologies, applications, and data-based tools. Additionally, the future smart society is data-based. The security of data implies security throughout its lifecycle. Aldabbas (Aldabbas et al. 2020b) defined a data lifecycle with five main processes: collection, communication, storage, usage, and destruction. The progression of the five phases does not have a linear nature necessarily. Some phases can overlap, but the beginning and ending stages are static. Most of the latest smart technology applications integrate the entire data lifecycle. Data security breach in any of the five phases causes damage throughout the entire lifecycle. Data must always be secured, every unauthorized access through any cycle stage must be detected and prevented, and the loophole that caused the breach requires fixing. Figure 2-8 shows the life cycle of data according to (Aldabbas et al. 2020b).

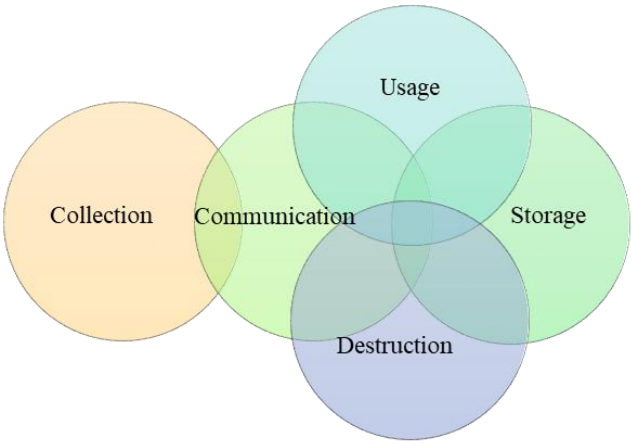


Figure 2-8: Data Lifecycle (Aldabbas et al. 2020b)

The data lifecycle starts with the first phase of data collection, which means gathering data and information to create value for the organization. This data is necessary for the operations of the organization. Data storage and maintenance is the next phase in the lifecycle. Data must be safely stored and maintained from external or internal harm or system failure shall that be hardware or software failure. Data must be easily accessible for use in the third stage, data

usage, and processing. The phase needs careful management, and access should be granted only to trusted and authorized users. The next phase is data communication. Data is communicated either internally or externally. Finally, data destruction is the phase where data must be terminally deleted when it has no further value to the organization. This task should be performed carefully and not underestimated, as data can be retrieved if the destruction is not executed properly.

In other data lifecycles in literature, Bloomberg names 7 phases to be the lifecycle for the data (Bloomberg 2015): 1) Data capture, which is equivalent to data collection. 2) Data maintenance. 3) Data synthesis. This term is not very common in the data lifecycle. It refers to creating data values by inductive logic and using other data as input. 4) Data usage also appears in (Aldabbas et al. 2020b). 5) Data publication that serves a similar purpose to data communication. 6) Data archival is not limited to data storage. 7) Data purging indicates the removal and destruction of data properly from the organization.

A look at the perspective of Wing (Wing 2019) to look at the data lifecycle displays eight linear phases, unlike the model of (Aldabbas et al. 2020b). Data generation, collection, processing, storage, management, analysis, visualization, and interpretation are steps. The model of Wing (Wing 2019) does not include data destruction or any data deletion. Hence, Wing speaks from a data science platform and focuses on extracting value from data rather than putting this data in its grave.

The service des ressources informationnelles et archives (UNIL 2019) at the University of Lausanne developed a vision for the data lifecycle. Their model suggests six linear phases for the data lifecycle:

1) Project management planning
2) Data collection or creation
3) Organization and analysis
4) Preservation and curation
5) Archiving and sharing
6) Reuse of data

This model sets certain goals: securing the storage through active phases, storing and using the data for the long term, and reaching a fair sharing of data that is non-commercial (UNIL

2019). However, the previous model (UNIL 2019) also neglected data destruction. Nevertheless, data deletion is present in most other literature, proving its significance. Consequently, data destruction should not be omitted or neglected.

Some specific types of data lifecycle are looked at in the literature-related data (Lange and Auer 2014). Linked data in simple meaning is a new method of spreading data on the web, which is particularly appropriate for machines and sharing information (Poblet et al. 2019). Lange (Lange and Auer 2014) discuss the lifecycle of linked data in their research and come to conclude that the phases for linked data are the following eight phases: revision and authorization, linking and fusion, classification, quality analysis, evolution and repair, exploration, extraction and data storage. These eight stages can influence each other. Figure 2-9 presents the linked data lifecycle according to (Lange and Auer 2014).

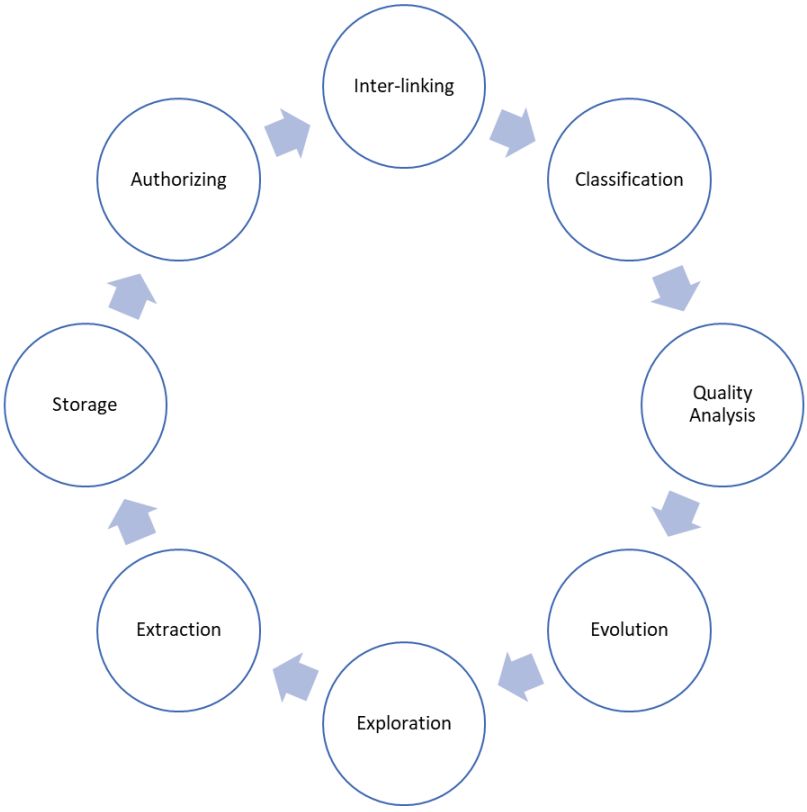


Figure 2-9: Linked-Data Lifecycle (Lange and Auer 2014)

To conclude, with data growing every second with unprecedented sources, companies are progressively pulling out value to present new opportunities for their clients. Nevertheless, there remains a problem with traditional data storage and process tools that are not competent to process all the information in the data. Big data are often centralized, making it more difficult for organizations to secure their data (Tankard 2012).

2.2.1.6 Social Security and National Security

As will be explained, the security concept deviates slightly from the concept. The terms of social security and national security come together because the origin of both is the United States of America. Both terms are addressed briefly in this dissertation.

2.2.1.6.1 Social Security

President Carter signed the amendments of the United States Congress that declared social security in 1977. Social security amendments aimed to balance the future of the public. Stabilizing the future means harmonizing the ratio of the pension to the average lifetime income (Brendler 2020). The national social security fund is engaged with several serious social issues. These are not limited to retirement pensions, medical insurance, unemployment financial support, work injuries insurance, and maternity insurance (Zhu and Zheng 2020). Afterward, the economy of the United States shifted substantially. Income inequality has risen dramatically while the population kept aging. There has been a bias in favor of young workers since. Four decades later, in 2018, counteraction movements pushed by the problem of the aged population, higher productivity risk, and high university education fees caused the alteration of the bias to favor older people (Brendler 2020). There have been no major changes in national security ever since, as (Brendler 2020) explains. Recently, the social security fund became one of the biggest investors in the capital market (Zhu and Zheng 2020). From the short presentation about the term social security, security in this context is a massive concept that concerns everyone's life in many ways. It does not present situational or instant protection for an individual against threat or danger. It is rather continuous protection for society for a lifetime. In other words, the center of social security is human welfare.

2.2.1.6.2 National Security: The Past and the Future

There is no harm in knowing the story of national security and how it reached its meaning. There has always been much ambiguity on the meaning of this symbol, "National Security". By the end of World War II, the terminology of national security was strongly established as a standard term alongside others like military affairs, foreign policy, and internal strategy. National security presents social development tied with a sovereign country as a kind of protection of its integrity (Grizold 1994).

Many scholars and publicists insist that foreign policy has to be dictated by the national interest and, more accurately, by the national security interest. In the 1950s, national security was used

together and sometimes coupled with national interest as (Wolfers 1952) clarifies. Both terms were used politically and gained popularity among policymakers and scholars. These political terms earned popularity among the people but did not necessarily mean the same things to everyone. They did not have a precise definition or a specific meaning at all. Everyone could label the policy he advocated with an attractive but deceptive name (Wolfers 1952).

Wolfers (Wolfers 1952) talks about the change in the interpretation of national interest in the last century in the United States. He says that national interest indicated supporting requests that endorsed the nation's best interest rather than separate individuals, but it was still vague and did not carry much more meaning. Right after the Great Depression that took place between 1929 and 1933, the headways of national interest were so much affected by the situation, and the question back then was whether the foreign policy of the United States should focus on filling the substantial needs of the sub-national level and pressure groups instead of promoting the welfare of the whole nation. People desired to see national policymakers widen their view of the narrow national interest perspective to go beyond economic development and focus on more inclusive interests. However, it was still hard to set standards to measure national welfare interest and define national interest.

Later in the 1950s, people's concern was that the policymakers might be overly concerned with the interest of the entire humankind and sacrifice the interest of the national community (Wolfers 1952). It is remarkable how public opinion can swing easily from one direction to the opposite in a few years under certain circumstances and from contentment to anxiety and fear. Afterward, the understanding of national interest shifted under the impact of the cold war and fears of external rivals more than internal fear like recession or social problems. Consequently, the symbol of national interest became synonymous with national security. National security became strongly established in political science and international relations. The general understanding of national security is protecting power. It often appeared by parties who rely on power rather than on confidence in behavior and international relationships (Wolfers 1952).

More recently than in the 1950 era, there has been a transition in the meaning and interpretation of national security. Since the end of the cold war era in 1990, redefining and reshaping the concept of national security was necessary due to the newly emerging political situation in the United States and Europe. The new form of national security will witness less importance for military forces while armed forces were always the dominant factor. An

alternative is improving the degree of collaboration between the countries to decide on mutual objectives to ensure the security of the society, states, and international community (Grizold 1994). Modern society after the cold war ended became more complex with new elements given more attention and relevance, such as economic factors, cultural importance, ecological issues, healthcare, and education. All these attributes contribute to shaping the new society, and consequently, the society's security must incorporate and embrace all these elements. Therefore, the term national security needs reconsideration. Grizold (Grizold 1994) stresses that this is achievable only by harmonizing the interests of the individuals and the state equally, in addition to their ties with the entire international community.

The national and international security terms need redefinition after the end of the cold war in 1991. Since then, many remarkable changes have appeared in the world, like rearranging the international community's power relations, which urges revisiting traditional concepts of international relations such as sovereignty, threats sources, and power balance.

The world needed higher levels of cooperation between the countries, especially the powerful countries, to solve or limit the consequences of clashes between some conflicting countries, plus the need to restructure a new order internationally. Restructuring a new national security system needed a new design to promote security strategy between the countries collectively. Amongst the actions necessary to achieve the new national security concept are limiting the military elements in the national security, reducing the budget for the armed forces, and reconstructing the international organizations established during the cold war (Grizold 1994). However, all these actions are only theoretical and hard to achieve without the commitment of the international community and the great nations.

National security, when used globally, indicates the security of the people in the nation and the relationships of the nation with other nations as well because in the modern interdependent world, the existence and the parish of the nation depend on their relations with other nations (Grizold 1994), especially on levels like the economy, diplomacy, and military.

National security is far from human security (Reveron and Savage 2020) and deviates from all security attributes discussed before. Nonetheless, national security is affected most of the time, especially in modern times, by similar actors that threaten human security, particularly cyber-attacks, as will follow later in this chapter.

National security term is purely political and defines a new dimension of security. The notion of national security for the U.S. is not limited to its borders. The 2002 strategy for national security implies that the United States has to defend liberty and justice because the values of liberty and justice are the rights of all people all over the world. In addition, the U.S. has obliged itself to advance human rights and human dignity in speech and actions (Bush 2009). A very simple question on this matter remains: what gives the U.S. the right to impose and defend their version of understanding of human rights on other nations and give them the right to intervene and violate other countries' sovereignty? Why not the other way around? Perhaps power is the only answer. Bush (Bush 2009) claims that the U.S. replaced tyrannies with democracy in Afghanistan and Iraq in 2002. The reality is that the wars Bush launched destroyed both countries to their very core in a way that is beyond repair. The U.S. indeed ended one kind of tyranny in these countries but also ended these countries.

For a long time, the nature of national security has been somewhat ambiguous (Wolfers 1952). Wolfers explains further the origin of this problem and the reason behind this vagueness: the regulating advice and norms that direct the national security strategy planning is vague and deluding. This advice needs to indicate what level of security the country wishes to achieve, by what means and methods it is feasible to reach, and under which circumstances. It is especially necessary to be cautious when designing a policy for national security, even if the solution seems very simple and backed up by the public because public opinion can swing rapidly from an end of contentment to the extreme opposite end of apprehension (Wolfers 1952). However, this was the old comprehension and the situation for national security before the cold war. Following the end of the cold war in 1990, the emerging situations in Europe and other parts of the world have increased the need to modify and redefine the content of the national security policies of modern countries. A new security structure was formed, in which the traditional role of military forces was reduced and implemented more widely. It is imperative to replace it with common security measures. Hence, the principle of armed security will no longer be the main factor for national security (Grizold 1994). The modern definition of the United Nations' national security indicates “the ability of a state to cater for the protection and defense of its citizenry” (Osisanya 2020).

In recent years, many conversations and discussions have arisen on how AI will affect countries' national security in both the long term and the short term. The talks came when the U.S. lost

some of its momentum and had the lower hand in terms of losing technological and scientific dominance to other nations like China which is expanding the investments in its research and development of new technologies (Briscoe and Fairbanks 2020). The major questions about the future of national security and AI are as (Briscoe and Fairbanks 2020) describe: how the evolution of AI will disrupt the current balance of powers between countries? Will AI be an essential element in future weaponry? Will the extended domains of AI pave the way for new grounds that are prone to attacks and need absolute protection? These matters gain increasing significance as the world rapidly adopts AI in most spheres preparing for the future. These trends are pushed not only by industry but also by most governments. Another important motive for countries to push for more AI is to improve their competitiveness, as China, Russia, and France are remarkably doing. The U.S. did not stand with its hands all tied up. President Trump signed an executive order in February 2019 to maintain America's superiority and leadership in AI (Briscoe and Fairbanks 2020).

Recent observations from a military standpoint in the United States on information security demonstrate why the foreign policy of the United States is being suffocated by the influence of the wide Russian operations like in Georgia and Ukraine, and the worldwide economic spying and surveillance by China, in addition to the increasing threats to what can be called digital human. The cause of these latest threats were hackers, cyber-criminal gangs, and massive attacks by independent groups and countries (Reveron and Savage 2020). The amount of pressure and danger is building up very quickly with time. Still, the response from the United States is going with slow movement because these growing challenges are not just crises, which makes it hard for the White House to react as they do in major terrorist incidents, for example. These observations show slow-marching challenges such as pandemic diseases, cyber-attacks, and growing land claims by Russia, which still has the Cold War mentality. There have been ago long warnings about the Covid-19 pandemic, but these voices were ignored not only by the United States. The health system in the United States can neither overcome the pandemic nor protect human security. This mentality reacts to challenges like cyber security, which confronts individuals, corporations, the government, and even the presidential elections (Reveron and Savage 2020).

Nevertheless, the United States did not reduce its spending on the military, and it continues with its research and developments in this field which makes the country very well prepared

for a conventional war (Reveron and Savage 2020). However, the threats that the United States is encountering are not as conventional risks are not only targeting individuals and corporations but also countries and governments are increasingly becoming a part of this whole digital war. High levels of interference are necessary to maintain an acceptable level of cyber security. To conclude, present and future security are going digital.

It is no longer possible to discuss national security without including digital security. Digital security extends beyond personal matters (Reveron and Savage 2020). As a society with all its components like the economy, communication, and education is shifting online, people in advanced countries are no longer isolated from the effects of cyber risks that now have more power to affect and impact land security and influence the people directly or indirectly. Opponents can now disrupt access to fundamental needs like electricity, communication, and even elections, as they can change people's perceptions about political issues (Reveron and Savage 2020). There are huge claims that a foreign country, namely Russia, had a foreign influence on the American presidential elections in 2016. Since then, U.S. intelligence has been deeply concerned with foreign activities on social media (Reveron and Savage 2020). Cyber attackers have developed new skills exploiting the psychology of the target and affecting their decision-making processes(Lin 2012). These new techniques are a simple illustration of the potential of cyber threats to national security. The US puts much effort into developing plans to limit foreign influence on the presidential elections in 2020 by regulating social media without limiting the freedom of speech and protecting platforms from exploitation. Nevertheless, there were beliefs that foreign adversaries would keep on their attempts to sway the voters' preference in the US to alter the foreign policy of the United States and weaken the confidence in democracy (ODNI 2020).

Advanced countries always try to enhance the security of the inhabitants through several actions that support the national security strategy, like protecting the borders, infrastructure, and cyber security. The efficiency of these measures might indicate to what level a country can protect its social values from threats (Grizold 1994), but these efforts will fall short if social development does not get its share of the investigation. Therefore, social development is an important element of modern social security and an essential factor for success.

National security structure is apparent in Figure 2-10 as per (Grizold 1994). For further insight into this structure, the reader is advised to read (Grizold 1994).

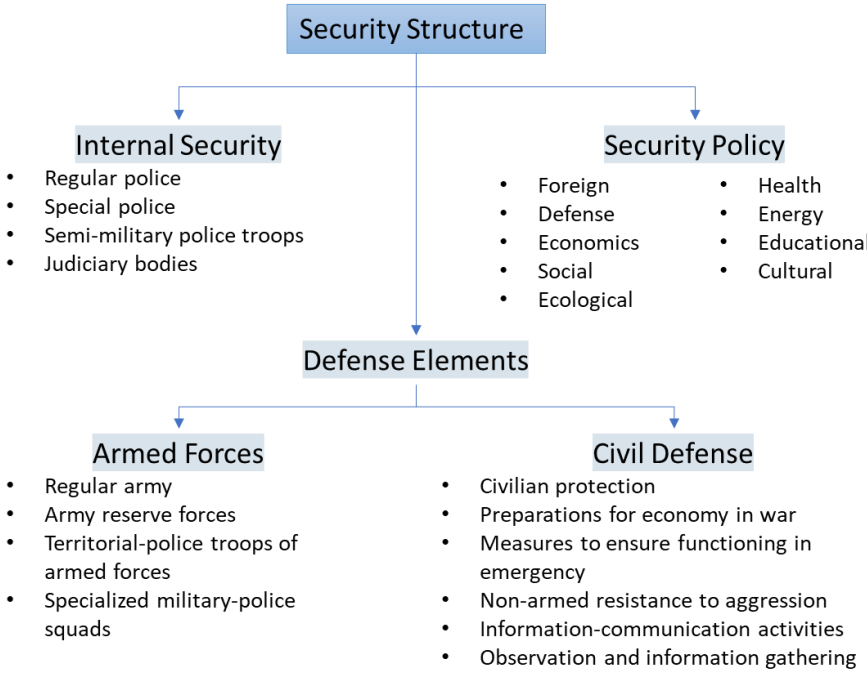


Figure 2-10: National Security System, adapted from (Grizold 1994)

2.2.2 Societal Security

Since the end of the Cold War, the term "social security" has received the greatest focus and is the subject of most discussion (Burgess and Mouhleb 2007). The rise of societal security resulted in a turn in security research toward culture, identity, and ethical conflicts. The definition of societal security is the protection of identity from a perceived threat, or more specifically, the protection of a community from perceived harm to its identity (WÆver 2008). The preservation of the values that make up and guide society is strongly related to that preservation. The absence of challenges to the values that society considers respected might be seen as security on a social level. Defining the values and ethics of a society is the simple beginning point of the investigation (Burgess and Mouhleb 2007). However, identifying national values is not an easy task, especially with the absence of clear expectations globally. In Swiss society, for instance, the most perceived values are neutrality, modesty, consensus, punctuality, egalitarianism, ethics, and humanity (Brühwiler et al. 2019). The most important definition of societal security is the definition proposed by the Copenhagen School of security studies: "the ability of a society to persist in its essential character under changing conditions and possible or actual threats" (WÆver and Carlton 1993).

After exploring different definitions of security and the various definitions of other security-related terms, not only to serve the purpose of this dissertation but also because it is a necessity to avoid confusion on the exact meaning and usage of the term “Societal Security”, the term societal security needs a definition in the context of smart society. So that when the term is mentioned, there should be no confusion about other security contexts. The definition of Societal Security is in Box 2-1.

Box 2-1: Societal Security Definition

> **Societal Security** is “protecting individuals and their values and ethics in a smart society from any risk and threat that is technology-related to meet human security needs”

Societal Security will be used in the context of Smart Sovereignty later, which makes it necessary to have a clear understanding of the term.

2.2.3 Conclusion

To date, science has not agreed on a universal agreement on broad definition of safety or security and there is no clear and direct justification for the vague definitions of security. Although many areas of science have developed their definitions of security, there are still efforts to arrive at a generally accepted definition. Nevertheless, it is important to stress that security expands to include national security and defending the country by armies or internal forces to control its citizens. The public policy proved to be necessary for security. The concept of security can include all the discussed subjects. However, this broad diversity in definitions and areas of implications will result in a society that does not have a clear understanding of what the definition of security is, especially with a conflict of interests for many parties. Therefore, security presents varying meanings and interpretations for different parties, depending on the time, location, and application context. Security has a capricious nature and vast fields and broad domains of applications, which gives it a multidimensional nature. The availability of decent definitions is necessary if one wishes to discuss security issues with clarity and accuracy. Despite the difficulty and almost impossibility of reaching a universally accepted definition of security, a concept of security can be defined when one certain context of application is selected. The terms accessibility, availability, and maintainability appear very

often in most security-related definitions. These three elements formulate the core of understanding the security concept.

The security of the future society requires more effort to guard. Digital human security, security of food, housing, energy, information security, cyber security, and data security are the domains that will see serious challenges and changes. A complete analysis of the challenges for future society will follow in chapter 3.

Societal security has a new definition which is modern and suitable for smart societies. This definition is necessary to answer research question number 3 (see Box 1-1 and Table 1.1) which makes it an important contribution of the dissertation.

As discussed in the introduction, Society 5.0 comes with a lot of advantages and opportunities for people in many ways. The following chapter 2.3 explores these promising prospects.

2.3 Opportunities for Society 5.0 and Industry 4.0

This chapter will briefly introduce some advantages the future Smart Society will bring thanks to the intensive cutting-edge technology application. However, the main aim of this chapter is to address the problems that accompany these technologies. Therefore, the challenges and threats accompanying technology are discussed in more detail than the advantages and opportunities. Afterward, the chapter will provide precise insights into AI technologies. Later, a section is dedicated to analyzing a series of interviews with selected experts on the matter at hand. Finally, a conclusion is drawn.

The ways technology growth will enhance civilization are many. Technology may lead to advancements like a greater standard of life and increased comfort. However, if it is not implemented correctly in society, it might also have adverse repercussions, such as negative effects on employment, uneven wealth, and knowledge distribution. Therefore, determining the ideal sort of society and directing growth in that direction is necessary (World Economic Forum 2019). The following paragraphs will discuss the potential opportunity areas.

2.3.1 Human Well-Being and Security

The main principle of the Society 5.0 is to handle social and economic issues in a coordinated manner while putting the needs and interests of humans first. Successful social equity and sustainable development initiatives must be created to accomplish this (Nagy and Hajrizi 2019). Ending poverty, preserving the environment, and ensuring prosperity for all are the objectives of Society 5.0, which was developed in consideration of the Sustainable Development Goals of the UN (SDG) (Shiroishi et al. 2018). A larger variety of stakeholders and digitalization technologies are very important since we have reached an era where the average lifetime of a person is approaching 100 years. The pursuit of genuine human security and well-being is just getting started. By expanding the number of individuals taking the initiative and changing the game, we can encourage a pioneering mindset and the capacity to be disruptive when necessary. It will be vital to pursue transformation through a collaborative ecosystem that combines ideas from business, academia, and people to quickly create a sustainable society on a global scale (Hitachi 2020). Security in Society 5.0 might be improved with integrated security solutions, for as by using AI technology to analyze pictures from surveillance cameras (Hitachi 2020). Implementing a quantum leap that would enable the creation of a super-smart society

and, as a result, let post-conflict nations recover from its effects more quickly would be very advantageous. The creation of affordable control systems to run specific alignment processes is essential to achieving Society 5.0 in post-conflict nations (Nagy and Hajrizi 2019).

2.3.2 Lifestyle Freedom

People will be liberated from various limitations that earlier hindered society and limited its freedom. People in Society 5.0 can pursue various lifestyles and beliefs and no longer have to prioritize efficiency (World Economic Forum 2019). Instead, attention is on meeting public needs, resolving issues, and adding value (Davidow 2018). Information will vanish, inequality brought on by the concentration of wealth (Atkinson 2016), and people will be able to contribute to society at any moment. In addition, Society 5.0 will reduce the threat and consequent worry posed by terrorism, natural catastrophes, and cyberattacks (Shiroishi et al. 2018).

Additionally, one of the basic Society 5.0 principles is protecting the privacy and freedom of people in a manner that guards and guarantees the equality and freedom of humans (Mavrodieva and Shaw 2020). With improved safety nets for unemployment and poverty, individuals may live in greater security (World Economic Forum 2019). People in Society 5.0 will also be free from resource and environmental restrictions, enabling them to live sustainably in any location. Everyone will have the opportunity to live, learn, and work without being subjected to restrictive forces that limit their identity, such as exclusion based on their beliefs and values (World Economic Forum 2019).

2.3.3 Healthcare Enhancement

Health, life expectancy, and quality of life will all rise thanks to Society 5.0 (Hitachi 2020). Healthcare in Society 5.0 will offer tailored and preventative treatment by gathering and analyzing individual health and medical data across the lifetime to enable individuals to live longer in excellent health and so contribute to the achievement of the third SDG (Fukuyama 2018; Clark and Wu 2016). The Federation of Japanese Business Organizations (Keidanren) is pleading with the government to provide the infrastructure to integrate health and medical data to make it accessible to different players and improve healthcare services (Hitachi 2020; World Economic Forum 2019). It is possible to guarantee long-term optimum health and a

higher standard of living by employing acquired data, both accumulated and real-time (Ioppolo et al. 2020). The ability of medical personnel to identify ailments more rapidly and administer the best therapy makes this feasible. Diagnostic imaging services that employ AI or community-based comprehensive care platforms are two potential remedies in Society 5.0 (Hitachi 2020). One such perspective strategy for the future revolutionization of healthcare is the employment of nanorobotics.

In nanomedicine, nanorobotics is a new, cutting-edge, and interdisciplinary discipline (Freitas 1999). In their nanoscale designs, nanorobots vary from macro-world robots (Requicha, Aristides AG 2003). Nanorobotic devices are similar in size to biological cells and organelles(Nelson and Dong 2010). These nanoelectromechanical devices can consistently and precisely carry out pre-programmed activities (Sierra et al. 2005; Bar-Cohen 2005). Nanorobots offer amazing promise in medical, biological, and pharmaceutical applications due to their small size and wide range of functional capabilities. One imagines a perfect nanorobotic system as self-organizing, self-replicating, and self-repairing (Frei et al. 2013). Viral vectors or extremely small virus-like particles may be used as carriers for medications, diagnostics, or other materials even if such a sophisticated artificial system may not yet be commercially accessible. Several more speculative nanorobotic systems have been developed to treat and diagnose different illnesses and disorders (Nelson and Dong 2010). The bottom line is that the means of healthcare offered by the most advanced technology have huge potential to reshape the healthcare systems around the globe in a better and more efficient way.

However, the costs of the modern healthcare system might not be completely affordable to everyone. Countries spend a considerable percentage of their GDP on healthcare. In the United States of America (USA), healthcare costs accounted for 17.1% of the GDP in 2013 (Squires & Andersons, 2015). The US spent 17.0 percent of its GDP on healthcare in 2019, while healthcare spending in Switzerland represented 2.1% of GDP in 2019 (OECD 2019b). These two nations have larger spending as a percentage of GDP than either Japan or Germany, which both have 11% or 11.7 percent, respectively. AI has enormous potential to lower healthcare costs and make healthcare, particularly preventative care, accessible to most people (Bernaert and Akpakwu 2018). Studies, for instance, demonstrate that engineers have to teach AI to identify skin cancer more accurately than humans (Scutti 2017). While there may be worries that AI may eventually replace doctors, recent research shows that it may be used to improve clinical

outcomes while relieving physicians of administrative duties. Of course, some concerns need solutions (Franceschini et al. 2021). Nowadays, health insurance companies typically pay the whole amount of the therapy that customers have to pay for without evaluating the service delivered or its need (Porter and Lee 2013). For instance, the electronic patient dossier (EPD) should help to accomplish shared decision-making and value-based care by including all parties engaged in the treatment process in quality measures (Hippisley-Cox et al. 2003; Spatz et al. 2017). Accurate performance measures across several healthcare providers are made possible by digital tools. Doctors will get less and less used to comprehending the fundamentals of technology as it becomes more sophisticated every day. Medical school programs should start including AI education and computational skills courses to prevent the widening knowledge gap between doctors and data science professionals. Only then can aspiring physicians be prepared for the upcoming oncology revolution (Franceschini et al. 2021).

The openness of the services offered is a key factor in determining quality. An important factor in improving the efficacy and efficiency of services is digitalization. The three aspects of "structural quality," "process quality," and "outcome quality" are often used to categorize the quality to be assessed in Quality Management (QM) in social and healthcare settings. Numerous elements of the three quality dimensions can improve with future digital support (Kuntsche and Börchers 2017). It is possible to demonstrate the rise in this characteristic mentioned earlier: The number of patients treated by many doctors who must take a variety of medications concurrently is growing due to the age pyramid shift and the age-related increase in chronic illnesses. The average number of prescriptions climbed by almost 26% during the past ten years (Atella et al. 2019). Knowing if patients have taken medicine recently and in what quantity is crucial in case of a referral, emergency, or unforeseen hospital stay (Wheeler et al. 2018). On transfer within a hospital, at least one in six patients may have a clinically significant medication difference (Duguid 2012). During a hospital stay, doctors often modify the medicine given to a patient, and after release, the patient can receive a new prescription for a different drug (Kerzman et al. 2005). If the patient takes both the newly prescribed prescription and the drug that was prescribed before his stay, this might result in a dangerous combination or an improper dosage with harmful side effects (Wheeler et al. 2018; Kerzman et al. 2005). The medication plan includes a summary of the medications given now

and is updated in case anything changes, which can enhance the experience of the patient greatly enhanced by this.

2.3.4 Mobility and Logistics

The objective of mobility and logistics in Society 5.0 is to offer dependable and secure transportation services to all. Autonomous vehicles have the potential to reduce congestion and traffic accidents significantly (Petrović et al. 2020). Such cars are dispatched in accordance with our lifestyle, for example, "Last mile" traffic solutions (Hitachi 2020). The future of transportation is revolutionized by autonomous cars. The productivity of the transportation system will be largely dissociated from ongoing human work in vehicles for the first time in human history. This promises significant decreases in the overall cost of travel and an increase in accessibility in response. New heights of economic expansion are anticipated as well as improvements in many people's standard of living. These benefits will be amplified further if drive time is converted to productive time and a sizable portion of the population becomes independent and mobile on their own. With the use of driving aids, autonomous cars can relieve drivers of tasks that are thought to be tiresome, difficult, or impossible, such as sitting in slow traffic or making lengthy highway trips (Bösch 2018). However, even with reduced per-vehicle-kilometer resource consumption and negative externalities, the size of the transportation system would still potentially lead to higher-than-ever traffic growth, induced demand, and related negative externalities. With autonomous cars having such a dual influence, it is important to consider what may be done to maximize their positive effects on society while minimizing their negative effects on the environment and society (Bösch 2018). There are also ethical problems when designing software for autonomous cars. Automated cars must adhere to technological performance requirements and conform to societal standards for human-to-human traffic conduct. The fundamental moral questions in philosophy and ethics serve as the foundation for societal standards, such as the avoidance of accidents and adherence to traffic rules. Therefore, engineers creating control algorithms for automated cars can gain from using philosophical ideas and frameworks to guide design choices. (Thornton et al. 2017).

The logistics industry has faced new problems due to global collaboration and the merging of online and offline channels. As a result, smart logistics has emerged as a viable alternative for

dealing with the growing complexity and volume of logistical operations. Technologies such as the IoT, information and communication technology, and AI make logistical operations more efficient. They do, however, alter the story of logistics management. This shift piqued academics' interest in engineering, logistics, transportation, and management (Feng and Ye 2021). Modern logistics firms rely on powerful and smart ICT systems to process and transfer information. Data access and information about the demand for logistics services and delivery alternatives are becoming more critical competitive factors for these organizations. Unfortunately, only the richest corporations can afford these complex technologies today. SMEs in the logistics industry have limited access to innovative and smart ICT solutions and the knowledge necessary to use them effectively. As a result, tools are needed to promote collaboration among smaller logistics businesses, which decreases transaction costs and has huge economic and environmental benefits (Kawa 2012). That is a strong possibility for the future of logistics in Society 5.0, and it, therefore, promotes sustainable growth.

2.3.5 Smart Cities

Beyond the smart city model, Society 5.0 seeks to create a super-smart society. However, it is crucial to comprehend and examine where and how the smart city strategy has developed, as well as how the idea of a smart city connects to Society 5.0 (Deguchi et al.). Modern "smart cities" seek to effectively manage every area, including rising urbanization, preserving the environment, energy consumption, and way of life. The idea is to develop people's capacity for effectively adapting and utilizing all contemporary ICT trends. The major focus is strengthening the urban core infrastructure and improving people's quality of life. The main goal of this research is to provide comprehensive background information on ML techniques and to examine the roles that ML, Deep Reinforcement Learning (DRL), and AI play in the creation of the smart city (Mehta et al. 2022). The answer to the electricity question measures smart cities. The decisive factor is the optimal use of technology to produce, consume and store electricity locally. The fact that end users are becoming producers too changes the energy market with the need for new concepts such as the Crowd Energy (CE) concept as a bottom-up approach (Teufel and Teufel 2014). The concept provides greater efficiency in energy use is possible through collective effort (Gstrein et al. 2016). However, smart cities are not only based on energy sharing. Smart Society extends to a smarter application in every aspect of daily life. For

instance, Social equity is a crucial goal that must be achieved to build a smart city (Okafor et al. 2022).

In smart cities, urban development is entering a new phase as pressures to decrease cities' carbon footprints rise in response to the climate crisis, the aging urban population in industrialized nations, and the concentration of people in cities in developing economies. These smart city solutions may apply to transportation, energy, recycling of resources, and water resources (Kohno et al. 2011). However, most of these benefits are realized if the people, who represent the real end users, are involved and can contribute during the whole design process of the smart city. The pertinent strategies for ensuring citizen engagement are divided into three groups: Citizens as co-creators, democratic contributors, and ICT users (Simonofski et al. 2019). New participatory methods that enable individuals to participate in formulating, executing, monitoring, and assessing public policy have produced an international trend toward more citizen involvement in policymaking and increasing interest in public participation in recent years (Granier and Kudo 2016). This citizen engagement has been put into practice in municipal and federal administrations and a wide range of other contexts (Rowe and Frewer 2005). ICT may be an effective instrument to encourage, improve, and even empower citizen engagement (Ishikawa 2002), for instance, by lowering participation costs by enabling individuals to join whenever and wherever they want through their smartphones (Marres 2016).

2.3.6 Sustainability and Infrastructure

Production may be planned in a super-smart society such that only the minimal amounts of the minimal products are created and supplied at the minimum times. Because of this, unnecessary production may stop, increasing environmental sustainability (Haanaes 2016). Turning knowledge and expertise into data is important, and then applying that data (Hitachi 2020). Sensors linked to the infrastructure (buildings, roads, bridges, river levels) allow for real-time monitoring of such infrastructure, which, for example, permits safe maintenance for anticipating infrastructure problems (Hitachi 2020). That is necessary, especially for Japan, a nation that will require significant expenditures on its physical infrastructure in the next decades. Additionally, in the event of disasters, the real-time data collected can identify or predict risky locations, and drones and robots can guide people to safety or provide them with essential supplies (Hitachi 2020).

Since the changes are already underway, it is imperative to find an answer as quickly as possible to how a society can best take advantage of all these potentials provided by Society 5.0. By providing an answer, one might assure that the present potential can be utilized as completely and effectively as feasible. Consequently, decision-makers from all industries might use the findings as a reference (e.g., government, and companies). Realizing Society 5.0 addresses numerous societal issues and is essential for attaining mid- and long-term growth (Khare et al. 2021). This realization requires integrating the innovations of the 4IR (IoT, big data, augmented reality, AI, robots, sharing economy) into every industry and aspect of daily life (Fukuyama 2018) and citizens' commitment and trust in their Smart Society.

2.3.7 Blockchain Technology

The way the world functions is changing due to new ICT. Modern society's problems, including poverty, migration, and challenges related to sustainable development, and governance, may be addressed with these technologies. Among these, blockchain stands out as a transformative technology that can create things in an entirely new and creative way, where there were none, they can provide answers (Mora et al. 2021). Even though the blockchain concept is often linked to digital currency like Bitcoin, its applicability in various situations and industries has been demonstrated via theoretical research and practical application (Teufel et al. 2019). Blockchain technologies have recently been the focus of intensive research and development by both businesses and academia (Mora et al. 2021). Several businesses, particularly those involved in the IoT and creative industries, are being impacted by blockchain technology.

The energy industry is amongst the most promising fields for implementing blockchain systems. Recently, blockchain's use in the recorded music industry has captured the interest of scholars (Turchet and Chan 2022). The blockchain might very well prove to be a successful solution to some of the significant issues of the present, such as a push towards decentralization/democratization, a need for more sustainable configurations, and increased resilience (Teufel et al. 2019). Blockchain is also used for public health care (Gul et al. 2021), and development programs (Merrell 2022). Rural communities are slowly becoming marginalized in a global economy where core/periphery theories of growth are prominent. Rural communities have tried decentralized government as a solution to this. However, this process is rife with institutional, financial, and political challenges. These frequently center on

problems with accountability and transparency and low participation rates. Blockchain technology may help solve the problems associated with decentralized government and even make rural regions more conducive to future innovation (Merrell 2022). Thanks to its exceptional qualities like enhanced security, transparency, and flexibility, blockchain energy have many benefits. However, this technology comes with many dangers and drawbacks, both at the system level, primarily affected by existing players in the energy industry, and at the technological level (Teufel et al. 2019; Teufel and Sentic 2022).

Problems and risks of Blockchain

Despite the maturity of Blockchain technology and that it has enormous promise, there are still substantial obstacles in the way of its general implementation. Blockchain is still prone to risks. For instance, Ethereum, the most well-known and developed programmable blockchain, is still vulnerable to several assaults. Smart contracts are susceptible to cyberattacks due to minor code mistakes (Teufel et al. 2019). The complicated process of blockchain integration software with existing systems is a fundamental issue associated with mainstream blockchain technology adoption (Prewett et al. 2020). The complexity of blockchain applications and the lack of standardization are also barriers to the prosperity of blockchain, in addition to the problem that businesses are expected to have difficulty hiring and maintaining people with the necessary skills and expertise to operate successfully with blockchain technology (Prewett et al. 2020).

One research (Chuang and Thomas 2010) lists three categories of risks: operational, cyber, and legal risks. The operational risks are data and identity theft, high transaction costs, a limited number of users, long-term experience, and applicants encountering technological difficulties. The cyber risks are that the interaction between the actual world and the blockchain world may be subject to fraud and blockchain is prone to hackers. The legal risks are tax fraud, illegal use of data and blockchain can be used to pay for illegal activities (Lu et al. 2019).

To summarize, blockchain does not solve security completely. While blockchain adoption is unavoidable for businesses, a hard evaluation of the risks and obstacles before, during, and after, blockchain deployment can assist assure long-term success (Prewett et al. 2020).

2.3.8 Conclusion

This subchapter discussed some of the most important opportunities and advantages of Society 5.0 which makes a great chance for advancements in every domain and impacts life positively in every possible aspect. However, a realistic view of Society 5.0 requires also a look at the other face of technology and the challenges it brings to security. The next chapter will provide a complete analysis of security matters in Society 5.0.

3 Analysis of Future Society's Security

After presenting Society 5.0 in chapter 2.1.5 Super-Smart Society, and Industry 4.0, and the massive range of advantages that it brings in chapter 2.3 Opportunities for Society 5.0 and Industry 4.0, it is time to explore the security issues that accompany the transition to Society 5.0 to have a full image about the future from a security perspective.

This chapter aims to provide a comprehensive three-approach analysis of the risks, threats, and challenges that will face society in the future. The first approach is presented in chapter 3.1 Theoretical Research: Challenges and Threats in Society 5.0 and Industry 4.0 which is about conducting theoretical research on the challenges and threats.

3.2 Qualitative analysis: Experts' Opinions on the Future presents the second approach of the analysis. Namely the qualitative analysis of interviews with experts in different fields. The purpose is to foresee future challenges from the perspective of businesses and to close the gaps between theory and practice. This knowledge is quite necessary, especially with experts in Swiss society.

The following section chapter 3.3 Quantitative Analysis: Forecasting Key Figures for the Future Society is one of the most challenging and important parts of this dissertation. The idea is to provide a solid forecast for the future based on historic data. Several forecasting methods are tested and applied.

Chapter 3 is the most important to answer research questions 1 and 2 (see Box 1-1 and Table 1.1 for details). The chapter's conclusion summarizes the answers, and Figure 3-1 presents the outlook of chapter 3.

Like chapter 2, this chapter is a long chapter with three long subchapters each of which focuses on one area of analysis. It is necessary to keep the summary and conclusions close to their respective subchapter rather than compacting the findings at the end of the chapter.

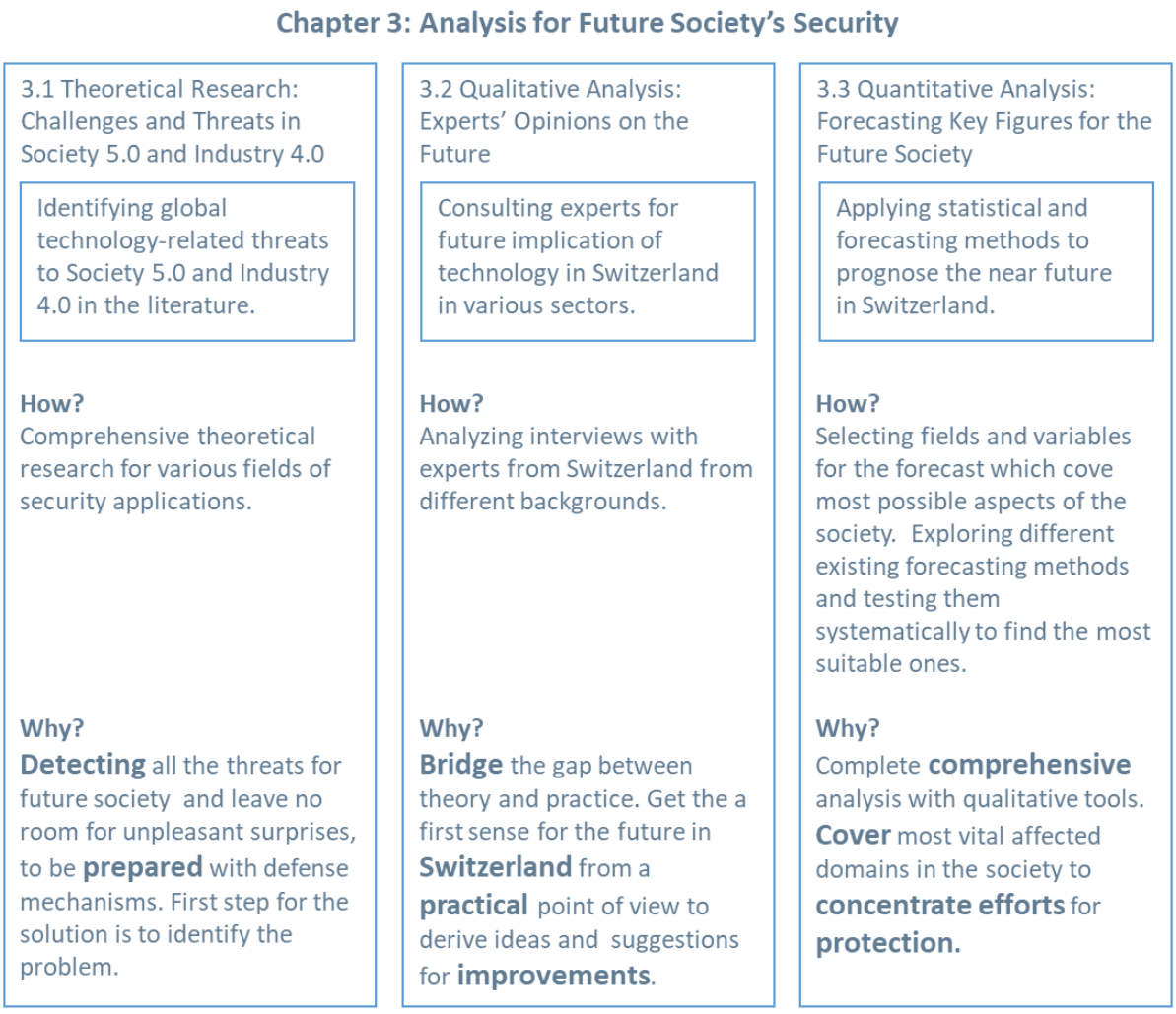


Figure 3-1: Chapter 3, Outlook

Since the early 2000s, many technologies have suddenly impacted our lives, led to major changes in our societies, and affected our understanding of communication and interaction with our surrounding medium. That strongly entails social media, which was unheard of before. These technologies with radical effects on society, industry, and the market are named disruptive innovations (Rahman et al. 2017). They carry changes in every domain, such as transportation, communication, research, and social life. Autonomous vehicles, blockchain, and the IoT have emerged. The modern world urges us to speed up the application and exploitation of these evolving technologies in every possible sector.

Additionally, global economic competition, social and cultural development, and efficiency purposes motivate corporations and governments to encourage digitalization to be applied in every possible societal domain. At the same time, individuals are rather motivated by the convenience of the technology itself (Warkentin and Willison 2009), which makes the influence

of digitalization on our everyday life immense. People are getting too dependent on almost every aspect of daily routine digitalization. People use preinstalled apps on their cellphones to easily monitor daily workouts, count how many steps they walk a week, and see how many calories they burn daily. The way people communicate with the world changed. Apps like Instagram, WhatsApp, and Telegram became essential and have completely locked most people in already. The comfort that technology brings does not come without a price. The price people pay for all these great services is not limited by any means to the monthly bills. It goes beyond that, as people pay with their privacy, data, information, media exposure, and sources of information.

The development speed of current technologies does not seem to slow down anytime soon. Many AI applications are seeing the light, while the development and maturity of these applications will need time. One should not underestimate the complex role of these technologies as society changes and possible challenges. Policymakers, academics, and the concerned individuals in society should be aware of this matter and need a good understanding of this phenomenon. Therefore, a deep analysis of the security of society in the future is required. This is done in this chapter and goes through three steps.

3.1 Theoretical Research: Challenges and Threats in Society 5.0 and Industry 4.0

Humanity is living in a tough time with rising levels of unpredictability and complexity (Fukuyama 2018). Global issues, including resource depletion, climate change, increased natural catastrophes, widening economic disparities, rising unemployment in certain industries, a shortage of competent people in others, security fraud, and terrorism are becoming more and more prevalent (Zhenmin 2020). So, it is essential to use ICT as effectively as possible. By connecting "people and things" and the "real" and "virtual" worlds (i.e., cyber-physical-social systems), it is possible to get new insights and generate new value using the fully realized potential of ICT (Wang et al. 2016; Shiroishi et al. 2018). That is a powerful strategy for addressing social concerns, guaranteeing environmental sustainability, improving people's lives, and maintaining strong economic growth (Da Costa Tavares and do Carmo Azevedo 2020). It would be necessary to address these issues by carefully involving diverse stakeholders to create such a society through digitization (United Nations 2019).

Each step of development in human society brings new barriers, challenges, and threats to society together with more prosperity. Humans will have to adjust and adapt to move forward and enjoy prosperity. The same applies to smart societies, as each stage of growth of the smart society has unique characteristics and areas of particularity from the security perspective. When examining security issues in current research, the emphasis cannot merely be on technology, as society needs a distinct viewpoint. Our security standards and individual views of security concepts must change and advance at the same rate to cope with modern needs and challenges. Higher standards and a better quality of life are brought about by rapid technological advancement (Aldabbas et al. 2020b).

There is a distinction between social risks and technical problems. Different risks and concerns are discussed (Aldabbas et al. 2020a). Table 3.1 summarizes the most distinguishable factors between technology and society concerns. The widespread reliance on cutting-edge technologies and the dependency on humans cause these distinctions. Societies have reached a point in human civilization when they heavily depend on these technologies. It is remarkably difficult to extricate society from the deeply rooted convenience and total dependence on the current modern system (Aldabbas et al. 2020b).

Table 3.1: Society and Technology Concerns, based on (Aldabbas et al. 2020a)

Concern for Society	**Concern for Technology**
Data protection	Heterogeneous data
Governmental surveillance	Hardware environment compatibility
Public manipulation	Security of data and cyber security
Unemployment	Digital trust and E-voting
Cyberbullying	Digital rights

It is necessary to understand that a smart society is a socio-technical system when discussing obstacles and difficulties for the future society (Vasauskaite et al. 2017). Therefore, considering only technical factors is insufficient; social qualities should also be carefully analyzed. A smart society is just as vulnerable as any other civilization from a social science standpoint. Since this civilization has certain traits and qualities, the process behind this susceptibility is distinct. The

issue here is that Society 5.0 is not immune to the typical dangers and threats that exist in everyday life.

On the other hand, a wise community is relatively receptive to new kinds of danger. Some hazards resemble those encountered in traditional society, but due to their distinctive characteristics and features, they are categorized as new risks and threats associated with the smart society (Aldabbas et al. 2020b). This society must overcome various obstacles as it moves toward and beyond Society 5.0. It is still difficult to create an all-encompassing system that seeks economic growth and answers various societal issues of different sorts to create a sustainable society (Shah 2008; Zhenmin 2020). The overarching goal is to bring about peace and prosperity for everyone and the earth by addressing issues with inclusion, leaving no one behind, and respecting all moral and ethical principles (Fukuyama 2018). Realizing such a society would depend on overcoming these obstacles through digitization and motivating many stakeholders at various levels to adopt a single future vision (Shiroishi et al. 2018).

Figure 3-2 presents the new technology-associated challenges for the future super-smart society. The threats generally fall into several categories (Aldabbas et al. 2020b). These are: Governmental control, cyber technology, global phenomena, and societal complexity are separated into these groups. There is a strong interaction between all the risk categories.

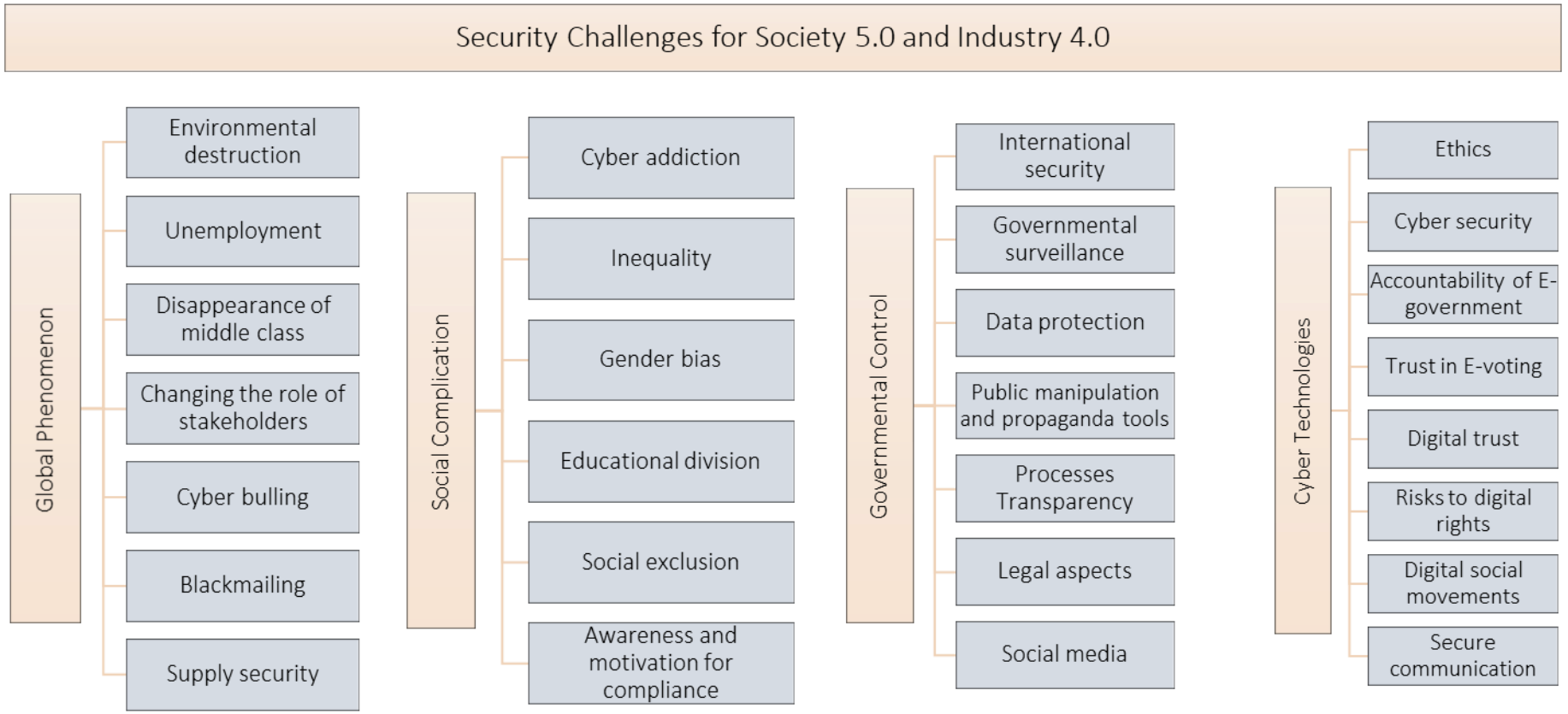


Figure 3-2: Risks and Challenges for Society 5.0

3.1.1 General Security Matters

Making security a priority in the coming Society 5.0 is a significant social concern. The adoption of enough security measures is necessary for Society 5.0 since a sizable quantity of personal data might be gathered and transmitted across networks. A highly intelligent society like Society 5.0 is just as susceptible as any previous society, i.e., Society 1.0 through Society 4.0 (Fukuyama 2018). However, the technique by which this susceptibility presents itself differs because this society's traits and attributes are distinct from those of earlier cultures. The drawback and issue here are that Society 5.0 is not immune to these common and well-known hazards and threats in traditional society.

In contrast, a wise society is relatively open and occasionally even more exposed to different kinds of danger. Some hazards resemble those encountered in traditional society 4, but due to their distinctive traits and qualities, they are categorized as new risks and threats, and therefore the task to overcome them arrives with Society 5.0 (Aldabbas et al. 2020b). The followings are some examples of serious security concerns:

3.1.1.1 Cyberbullying

The current emergence of cyberbullying is a new type of harassment and bullying (Slonje and Smith 2008). Cyberbullying may fall under various areas via text messages, phone calls, and, most importantly, social media. Cyberbullying has a very harmful effect on children, and as cyber-victims frequently decide not to inform anybody about it, adults may not be aware of it. Adults also experience cyberbullying (Slonje and Smith 2008). Data security concerning the risk of cyberbullying is a major issue of concern in the transition to Society 5.0 because of the large quantity of personal data that may be gathered and shared across systems in Society 5.0. Although widely used, social media be a double-edged sword for users (Giumetti and Kowalski 2022). Positively, social media reduces the distance between friends and family members, making it easier to uphold current ties and forge new ones (Bayer et al. 2020). On the other side, using social media can result in cyberbullying, negatively affecting both victims' and offenders' well-being, including strained relationships and increased psychological discomfort (Giumetti and Kowalski 2022). Potential remedies are possible by comprehending the online behaviors and individual differences most likely to cause cyberbullying victimization and

perpetration. However, victims must also be aware of the best solutions, and observers must be urged to act to protect the victims (Giumetti and Kowalski 2022).

3.1.1.2 Blackmailing

Blackmailing is often addressed with cyberbullying (Tanrikulu and Erdur-Baker 2021; Haider et al. 2022). The difference here is that attackers are increasingly threatening corporations, enterprises, and organizations with blackmail by attempting to encrypt and then expose their corporate data on public websites if the targeted entity does not agree to make payments for them (CERN 2020). Data collection and sharing across platforms will characterize Society 5.0, which naturally creates security concerns and offers more ground for cyber-criminals.

3.1.1.3 Social Exclusion

The process by which people are denied or underprivileged full access to a range of rights, opportunities, and resources that are typically available to members of another group and that are essential to social integration and respect for human rights within that particular group is known as social exclusion or marginalization (Silver 2007; Peace 2001). Alienation or deprivation of citizenship due to social exclusion may be connected to a person's socioeconomic class, nationality, religion, ethnicity, and level of education. (US Department of Health and Human Services 1999). In a future super-smart society, the immense power of social media carries several potential risks, including the possibility of social exclusion beginning to emerge (Aldabbas et al. 2020b). One misinterpreted post or tweet can have serious, irrevocable effects and further ramifications on the life of the victims in cyberspaces like Twitter, for instance.

3.1.1.4 Secure Communication

Confidentiality and integrity are closely tied to this security issue in the context of secure communication. To maintain data security in data transfer and storage, many encryption methods, such as homomorphic encryption technology, are now in use (Aldabbas et al. 2020b). Using homomorphic encryption, sensitive data may be safely sent between computer systems and stored there (Ogburn et al. 2013). However, the advent of quantum computing and the resulting surge in computing power (Miller 2019) have made it difficult for conventional

encryption techniques and even blockchain technology to provide data confidentiality and secure communication in the face of such a powerful computer environment (Arute et al. 2019).

3.1.1.5 Supply Security

Global supply chains are experiencing significant disruptions and challenges as they attempt to adapt to the brand-new requirements of a locked-down world. In today's complicated and internationally networked world, independence and security of supply are especially important in several industries connection between supply chain operations and the continuing Covid-19 outbreak has been broadly discussed. The core of the discussions is the relationship between the present worldwide shortages of important items, such as medicine, and supply chain problems, such as a lack of supply chain resilience and transparency, as well as unsustainable just-in-time production. To lessen the consequences of these problems and safeguard supply chain operations, measures such as implementing a plus-one diversification strategy, nationalizing medical supply chains, and boosting safety stock need to be taken. These suggestions are made to lessen the effects of the crisis now while also giving businesses the resilience they need to deal with future shortages that may be comparable (Zhu et al. 2020). Other precautions can be implemented to limit such shortages in the future, but these are not always simple to apply without more collaboration between the international players (Park et al. 2020). The necessary collaboration to overcome the uncertainties and supply shortage has geological and geographical barriers (McNulty and Jowitt 2021).

3.1.1.6 Digital Addiction

Online gaming and smartphone addiction, are driven by cyber technologies and contain the risk of addiction. However, these very technologies are possibly able to offer new intervention techniques to treat addiction (Takahashi 2018). Hence that the problem of internet addiction has long been recognized and searched (Young 1998) and the concept of "Internet addiction" was discussed in 1995 (Takahashi 2018). Researchers found that excessive exposure to and use of video games and social media, especially Facebook, cause unprecedented cyber addiction (Suissa 2015). This addiction occurs when users are too afraid to be disconnected from social media because they risk missing important things (Nadkarni and Hofmann 2012). However, some cyber technologies and AI can help analyze and treat addiction disorder by

improvements of data collection and data analysis in addition to enhancing the diagnosis and classification of patients (Takahashi 2018).

3.1.2 Privatization of Digitalization

In the digital age, patterns of competitive and monopolistic behavior, market power arrangements, and instruments of interfirm connections are undergoing profound alteration. New monopolistic tactics emerge to create, develop, and maintain market hegemony in diverse sectors (Rozanova 2021). The Google (Alphabet), Amazon, Facebook, Apple, and Microsoft (GAFAM) market capitalization is an astonishing example.

Privatization of knowledge, information infrastructure, and market access is the result of the "privatization of digitalization." Concentration and monopolies result from network effects. As a result, the knowledge society's potential is not being realized, the economic benefits of digitalization are not being fully realized, and a concentration of power is growing within huge technological organizations (Allam 2020). Following significant expansion between 2010 and 2020, GAFAM are among the world's top ten corporations in market value. GAFAM stands for "Big Five" technological corporations, commonly known as "Big Tech" (Human and Cech 2021). The market value of the five Big Tech companies GAFAM exceeds the GDP of Japan, Germany, and France (individually and not combined) (Guitton 2022), demonstrating the notable power concentration within these corporations.

3.1.3 Social Media

For each firm, social media presents both possibilities and hazards. The secure integration of social media platforms into organizational ICT infrastructures is primarily concerned with technical considerations. Social media security management often overlooks the human factor, yet protection can only be delivered through a comprehensive strategy. The culture of social media security must be integrated into the entire corporate culture (Oehri and Teufel 2012). The matter gains more significance by the day as the spread of social media use grows constantly, unlike the awareness of the consequences. It is hardly unexpected that the Covid-19 pandemic generates a lot of social media buzz. There was an alarming lack of cyber security talks. Recent data breaches and ransomware incidents indicate that firms should devote more time to discussing risks and mitigations. Only 12% of tweets on the IoT mentioned themes like

encryption, vulnerabilities, or risk, among other cybersecurity-related phrases (Scheibmeir and Malaiya 2021). The future society will need more IoT cyber security communication and planning. The IoT announced implicitly a modern age of computing through which every conceivable object is fitted with or linked to a smart device that makes it possible for data gathering and interaction over the internet. However, the IoT confronts personal privacy from the perspective of the data collection and usage of individuals' personal information. Scientific research reveals four fundamental confidentiality topics embody problems associated with collecting personal information through the IoT. These are unauthorized surveillance, uncontrolled data generation, and use, inadequate authentication, and information security risks (Caron et al. 2016).

Members of online social networks are growing every day, and at the same time, assaults and threats against users of these networks are also growing (Cengiz et al. 2022). Social media is posing an increasing existential danger. People express their commitment to domestic tranquility, common defense, and general welfare under the constitution to guarantee the benefits of liberty. As a result, policymakers are tasked to ensure that social media is secure, accessible, and useable by all. Currently, social media businesses and their platforms constitute a threat to national security and the nation's societal fabric. Social media is no more just a tool for connecting communities and individuals. It is increasingly used to disrupt and undermine trust in our democratic republic, its people, systems, and institutions. Citizens, public and private groups, elected officials, alternative media, and others can publish, post, and promote misleading-to-false information via various social media platforms without repercussions (Hernandez 2021). It is too much of a powerful weapon to keep the power of social media in the hands of a few persons who directly and indirectly force their values and beliefs on the social communities and, more dangerously to the freedom of people, their political agenda. Political polarization is a problem that society will probably face in the near future, and social media is exploited for that. The fragmentation of the news media and the propagation of false information on social media are some of the causes of the rise in political polarization (Kubin and Sikorski 2021).

Moreover, social media has grown in importance in democratic decision-making processes like elections or referendums. The exploitation of social media in attempts to sway public opinion and affect outcomes, compromising the principles of democracy, has come under scrutiny in

recent studies. There are analyses and empirical data regarding how social media affects political campaigns (Saldivar et al. 2022). Astonishingly, the single determiner of content and user reach is social media firms, who are shielded from liabilities of the intended or unintentional repercussions of material found or shared via their platforms by some regulations and liability safeguards (Hernandez 2021). Facebook and co (in other words, Mark and Jack) should not be allowed to force their community regulations and what they claim to be freedom of speech on users all over the globe. The phenomenon that everyone who is not a liberal will be eventually banned from Facebook and Twitter must stop. Reforming social media laws is necessary because of the risks connected with its current usage. Social media is a dangerous instrument that may cause pain, damage, and physical and emotional causalities, bypassing, usurping, and undermining society's values (Hernandez 2021). Social media has dangers for teenagers, ranging from widespread problems such as polarization and digital addiction. At both the individual and social levels, the entire impact of the existing social media platform architecture necessitates a thorough assessment and conceptual advancement. Combining algorithmic and instructional approaches that avoid pushing users' cognitive boundaries and include community welfare is part of the answer to enhancing the effect of social media (Ognibene et al. 2021). Social media failed societies once more when it failed to filter and fight the spreading of fake news and conspiracy theories in the era of the Covid-19 pandemic. The future pandemic may be deadlier and spread more swiftly. Social scientists must draw lessons from the 2019 pandemic to ensure that epidemiologists and medical professionals worldwide may work as effectively as possible without being hampered by illogical but predictable actions (Craig and Sadovykh 2022).

3.1.4 Spying

Many advanced software developers go beyond just hacking. They sell their products to governments to practice illegal and unethical espionage and surveillance of their citizens.

The Israeli-developed Pegasus, widely regarded as the most sophisticated mobile spyware in the world, is available for both iPhone Operating System (iOS) and Android smartphones. The malware has developed further since it was first discovered (Schless 2022). The ability to offer the malicious actor full control over the victim's device, the data it can harvest, and the development of Pegasus into a zero-click payload all contribute to its high level of

sophistication. From applications like WhatsApp and Signal, Pegasus can extract incredibly precise GPS locations, pictures, email attachments, and encrypted chats. Additionally, it may activate the camera to capture video and the microphone to listen in on private phone calls or in-room chats (Schless 2022).

Pegasus has demonstrated how simple it is for governments to spy on citizens nowadays. Due to the prevalence of these instruments, there have been proposals for legislation to keep them under democratic control. News has been dominated by the revelation that Pegasus was used to track human rights activists, journalists, lawyers, and many other people around the world, including in India and other nations like Azerbaijan, Bahrain, Hungary, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, and the UAE (Mehrotra and Bhardwaj 2021).

The NSO Group (an Israeli IT company well known for its tailored malware Pegasus) has been denying for a long time that Pegasus is utilized by bad actors. According to the business, Pegasus is only sold to law enforcement and intelligence agencies of around 40 different nations, and every prospective customer has had their human rights records thoroughly investigated. Not only government organizations, but all individuals should be alarmed by this disclosure about how extensively utilized Pegasus malware is. Similar to phishing techniques, the commercialization of spyware puts everyone in danger (Schless 2022).

The problem is not Pegasus itself. It is the systematic governmental attitude toward spying and harassing citizens under names like "fighting terrorism" or "national security" and many other claims. There are countless examples of such violations. Without a question, Pegasus is a mechanism that aids authoritarian governments in achieving and upholding their objectives. For this reason alone, one cannot immediately conclude that this system is also in line with the requirements and expectations of democracies, particularly that its application does not threaten the caliber of standards set in the domain of legal interference with basic rights (Rojszczak 2021). The introduction of advanced surveillance methods, such as Pegasus, must also entail a review of current legislative rules to guarantee that the use of these products increased capabilities is properly controlled and under the law (Rojszczak 2021).

3.1.5 Ethical Challenges

The philosophy of morality known as ethics reflects human behavior in the conflict between obligation and freedom. Freedom is defined as the lack of limits on behavior in a negative meaning and allowing action in a positive sense (Düwell et al. 2011). Competencies place restrictions on positive freedom since, without them, actions are impossible. Social norms and legal restrictions that forbid or considerably restrict courses of behavior under the prospect of negative consequences are where negative freedom is constrained possible to go around normative criteria, but doing so frequently has unfavorable effects. Several legal limits apply to the creation of software, such as copyright laws that prohibit the copying of source code or data protection laws that require the security of personal information.

The information revolution has largely affected the ethics of our communities since 1960. The revolution has considerably changed numerous characteristics and perspectives of our life in fields like trade, work, healthcare, safety, transport, and leisure. Modern ICT caused positive and negative changes in our communities and our relationships with each other life (Bynum 2015). The international understanding of freedom and democracy has also been challenged in most communities. That is only one small example of the ethical influence of modern ICT systems. The phrase "computer ethics" has been used for quite a while now in many different directions. For instance, ethics reflected the application of traditional ethical theories like Utilitarianism, deontology, virtue ethics, natural law, and such to ethical issues that substantially revolve around the use of ICT (Bynum 2015). The meaning of computer ethics is related to applying professional conduct in the computational sphere and employing codes and standards of good practice within the programming industry (Bynum 2015). More recently, the changes in our life in the modern world with its advanced technologies are shifting the focus and research of ethics studies for society into the direction of data ethics and its branches. The concerns in modern research are solving moral problems and improving human principles and values, so they get their right position in the future society. When we speak of data, this should include the data's lifecycle and its users' benefit. The stages start with generating and creating data, registering and saving data, processing and managing data, distributing and sharing data, and finally, using the data. The ethical question of algorithms is growing problematically in the scientific debates. AI, ML, robotics, and IoT are all carrying up, to a certain extent, the same implications in society and the industry. The real problem is not

in technology but rather in the subsequently created applications of the technology. That has provoked discussions about responsible innovation, ethical programming, and the need for best practices to support the right conduct and values (Floridi and Taddeo 2016).

Technology research needs to focus more on the different moral dimensions of all sorts of data, algorithms, and their applications. Sometimes, the data might not transfer into information, but it can motivate certain behaviors. Therefore, it also should be counted in the circle of focus (Floridi and Taddeo 2016). Technological giants ought to analyze the ethical implications of their products and how to improve the nature of the interaction between the algorithmic processes and the end users, instead of only innovating in digital technology and letting society live with the consequences. There is a moral obligation and liability of developers, programmers, and computer scientists about unpredicted and unsought consequences of data and algorithms and the lost opportunities (Floridi 2016a). Ethical challenges created by data and algorithms are very complex. Due to this complexity, tangible improvements for society when speaking of ethics and values can only be seen if ethics for data and algorithms are integrated from the beginning on a macro-ethics level. There is a need for a holistic framework to avert tight, ad hoc approaches and focus on the ethical effect and repercussions of data and AI in a coherent, holistic and comprehensive framework (Floridi and Taddeo 2016).

3.1.6 International Security Challenges

The future challenges in terms of international security in the context of direct and indirect clashes between countries gain more importance as the means of war have more potential damage thanks to implementing technologies in the arms industry. Emerging technologies are transforming security. Schwab (Schwab 2016) elaborates on these security problems and treats them as a threat carried with Industry 4.0. Drones: They resemble flying robots in many ways. The US now holds the top spot, but technology is becoming more accessible and less expensive. Autonomous weapons, which are armed with AI and drone technology, can choose and engage targets based on predetermined criteria without human participation. Space is becoming increasingly militarized, even though more than half of all satellites are used for commercial communications.

Additionally, a new generation of hypersonic "glide" weapons is about to enter this field, raising concerns about the inadequacy of the present procedures for controlling space activity and enhancing the likelihood that future wars may involve space. Wearable technologies can improve performance and health in situations of great stress or create exoskeletons that improve soldiers' performance and enable a person to lift loads of up to 90 kg without a problem. Additive manufacturing will completely transform supply chains by allowing replacement components to be produced on-site from digitally transmitted blueprints and locally accessible materials. Additionally, it could make it possible to create new warhead designs with better detonation and particle size control. Local power generation made possible by renewable energy is altering supply chains and improving the ability to print components on demand, even in remote areas. Metamaterials are being created due to nanotechnology or intelligent materials with characteristics that do not naturally arise. It will eventually lead to systems that can self-replicate and assemble, making weapons better, lighter, more mobile, intelligent, and precise. The history of biological warfare predates combat itself, yet quick developments in biotechnology, genetics, and genomics portend the development of brand-new, incredibly dangerous weapons. Potential apocalyptic scenarios are based on airborne designer viruses, created superbugs, genetically modified diseases, and more. Like biological weapons, technical advancement makes the construction of biochemical weapons virtually as simple as a do-it-yourself project, and drones might deliver them. Social media: While digital platforms offer chances for disseminating knowledge and coordinating efforts for charitable causes, extremist groups may also utilize them to recruit and organize supporters, as was the case with the Islamic State (IS). Young adults are more at risk, especially if they do not have a strong social support system.

3.1.7 Job Security

New enterprises will arise, and existing businesses will thrive because of sophisticated technologies that will be implemented (Schmandt et al. 2019). Still, as things have always been, technology will generate new job opportunities, but it will make many existing jobs redundant, and eventually, these jobs will be eliminated (Rumberger 1984). The possibility of losing many jobs will have a serious negative effect on society, and more disadvantages for the middle in a course, on the bright side, creating advanced technologies and implementing them in the

future society may have many beneficial effects when it comes down to an improvement in productivity, competitiveness, and reducing expenses.

The latter statement raises two key questions: can technology generate more jobs than it demolishes? Does technology generate more highly skilled jobs than it demolishes (Rumberger 1984)? Before examining these two questions, it is important to note that technological innovations do not necessarily behave similarly when they impact society. In the past, laborers had a lot of physical tasks, and their force destined their job. Consequently, with technological advances, most of these jobs were lost and replaced by machines.

Nevertheless, the economies witnessed waves of unprecedented growth, creating even more jobs than lost ones (Rumberger 1984). The labor workers were able to find new jobs as a result. However, our modern technology has proved to increase productivity and simultaneously reduce dependence on existing labor forces. People considered skilled and well-educated find themselves without jobs in many societies in most areas of the economy.

Meanwhile, persistent rises in productivity can restrict the capability of the economy to create sufficient new jobs to compensate for those demolished jobs by technology (Rumberger 1984). Some modern researchers suppose that technologies would unlikely be able to create new jobs and assist in cutting down current unemployment rates (Graetz and Michaels 2017). Other pessimists predict that society will suffer from the disadvantages of demolished jobs far more than it will enjoy the advantages of created jobs. That indicates that the risk of unemployment because of technology needs to be considered and studied deeply and carefully.

One of the most concerning problems with Society 5.0 is that AI technology will be able to take over many human professions. If the ethical challenges of AI are not addressed before unemployment becomes a severe social issue, considerable social upheaval may result (Su 2018). In some ways, AI has already exceeded human skills. Deep Blue, an IBM supercomputer, defeated world chess champion, Garry Kasparov, in 1997 (Newborn 2012). Many jobs were lost during the 1960s and 1980s due to automation and outsourcing to low-cost countries (Su 2018). The United States "Rust Belt" results from enormous employment loss. The downward spiral of harm resulted in the loss of 50,000 jobs in Youngstown, Ohio, over five years when numerous steel factories shuttered (High 2002). Suicide and divorce rates rose during this period, and the city became the homicide capital of the United States in the late 1980s, with the city's population decreasing from 170,000 to around 65,000.

As a result of this event, many workers felt excluded and as though they no longer had a voice in public policy, commercial interests, or government (Gest 2016). The advancement of AI technology will be the new driver of the old and ongoing process of work automation, which is the fundamental automation technology used to substitute people (Su 2018). Exoskeletons, collaborative and mobile robots, and other rapidly developing automation technologies, like in the previous era, can enhance working conditions while posing threats to disrupt the manufacturing industry (National Academies of Sciences, Engineering, and Medicine 2017). For example, industrial robots are broadly utilized in car manufacturing lines in North America, Europe, Japan, and South Korea and have eliminated or displaced a substantial number of employments there (Coffey and Thornley 2006; Su 2018).

The automation of occupations will speed up much faster with AI and will also have a wider impact. That is because typical automation needs explicit programming, which necessitates a significant amount of human effort and thus raises manufacturing costs (Brogårdh 2007). ML, in contrast, may be used by AI without explicit programming since it evolves based on the actual data it gathers via experience (Ortner and Leitgeb 2011). Through constant trial-and-error procedures and repetitive training, AI skills may be significantly and quickly enhanced. A technique of learning this potent may be simply adapted to many aspects of life (Su 2018). In general object identification contests, modern deep learning-based picture recognition techniques are far better than earlier methods (Fujiyoshi et al. 2019). A wide range of professional industries, including transportation and logistics, office and administrative assistance, personal and home services, accountancy, and construction, are impacted by the use of AI (Su 2018). Many academics assert that automation, especially via the employment of robots, will create jobs for people (Freddi 2018). However, the employment losses brought on by the consequences of robotics are far more serious (Aldabbas et al. 2020b), or at the very least challenging for future job seekers as new sorts of talents will be needed in manufacturing in the future due to the qualitative changes in the labor market, particularly in service offering and software development (Freddi 2018).

Many studies are predicting the impact of automation on the job market. MIT Technology Review made a summary of these studies in terms of jobs created and jobs lost and gathered the findings in Table 3.2 (Winick 25-Jan-18).

Table 3.2: Impact of Automation on the Job Market (Winick 25-Jan-18)

When	Where	Jobs Destroyed	Jobs Created	Predictor
2016	worldwide		900,000 to 1,500,000	Metra Martech
2018	US jobs	13,852,530*	3,078,340*	Forrester
2020	worldwide		1,000,000-2,000,000	Metra Martech
2020	worldwide	1,800,000	2,300,000	Gartner
2020	sampling of 15 countries	7,100,000	2,000,000	WEF
2021	worldwide		1,900,000-3,500,000	The International Federation of Robotics
2021	US jobs	9,108,900*		Forrester
2022	worldwide	1,000,000,000		Thomas Frey
2025	US jobs	24,186,240*	13,604,760*	Forrester
2025	US jobs	3,400,000		ScienceAlert
2027	US jobs	24,700,000	14,900,000	Forrester
2030	worldwide	2,000,000,000		Thomas Frey
2030	worldwide	400,000,000-800,000,000	555,000,000-890,000,000	McKinsey
2030	US jobs	58,164,320*		PWC
2035	US jobs	80,000,000		Bank of England
2035	UK jobs	15,000,000		Bank of England
No Date	US jobs	13,594,320*		OECD
No Date	UK jobs	13,700,000		IPPR
				*** estimated**

The numbers in Table 3.2 show that the rate of destroying jobs is almost two times higher than the rate of creating them. This rate will disrupt most economies and will cause serious social problems in the next few decades. Despite that, these are mostly estimations and have their limitations, governments, and social and labor organizations should be worried and plan to prepare for the future. Despite that some researchers think that automation is not expected to destroy too many jobs soon, the digital revolution will significantly impact the economy by creating the polarity in the job market. Up till now, technology is not capable of automating jobs that require low skills especially jobs that need social interaction and communication, and jobs that require certain physical motions. ICT will damage a broad range of routine jobs and some basic industrial production jobs. Additionally, it will generate new high-skill jobs and tasks that involve learning abilities and IT skills that machines and robots will not be able to deliver (Vardi 2015). We already see increased demand for ICT employees in most industries. In the future, people with lower IT skills will suffer, the income gap will increase among workers in society, and more pressure will apply to the middle class (Vardi 2015).

3.1.8 Artificial Intelligence and New Horizons

AI will speed up the automation of most tasks in several industries worldwide. It is also expected to result in fundamental global unemployment, as discussed before. Robotics will grow so universal that many skilled workers today will not find new jobs depending only on their current skills. Many opportunities will emerge for existing and future emerging companies, but challenges will also appear. In the past, technology instigated unemployment, which severely consequences society and the economy. Companies, governments, and public organizations must examine methods to create jobs instead of the ones destroyed by AI and reconstruct the damage to society. A future smart society will necessitate strategies and policies to reduce unemployment. They involve reforming education, enhancing governmental training programs that offer education and support to workers, merging AI and humans to execute tasks, pushing down the costs of health care and living costs in general, and preserving the AI industry's productivity (Su 2018).

A primary question should come into the discussion before starting the talk about what AI brings to the community and before diving into ethical debates and browsing the drawbacks of AI on society. Before posing the question, it is necessary to know that AI is not only a

technological change. It also comes with a cultural change (Bentley and O'Brien 2017). The question that needs an answer is "What is an appropriate role for AI?" (Cukurova et al. 2019). The opposing arguments here are whether AI should be an assistance to humans and help humans develop intellectually, or should AI replace humans as it can perform tasks that humans cannot. This dilemma applies in most domains that AI appears in, such as education, healthcare, and decision-making.

The OECD suggestion includes five complementary values-based principles for responsible AI governance (OECD 2019a). Table 3.3 presents these principles.

Table 3.3: AI Principles, based on (OECD 2019a)

#	Principle	Explanation
1	Inclusive growth, sustainable development, and well-being	AI should be trustworthy for all individuals, society, and the planet
2	Human-centered values and fairness	The design of AI must respect laws, democracy, and human values to reach a safe and just society
3	Transparency and ability for explanation	AI design should enable people to understand it and be transparent and responsible
4	Robustness, security, and safety	AI systems must be robust and safe all the time with regular assessment and management
5	Accountability	Developers of AI are accountable for the proper functioning of AI systems

3.1.8.1 The Importance of AI for Life and Science

The new forms of AI applications, such as deep learning, allow humans to learn new approaches to difficult problems. AI can make us smarter because it works very differently than we do and can process vast amounts of data we can never oversee ourselves. Such systems may be able to alert us to our own biases and systematic errors. AI allows us to mirror ourselves in it. AI does not take decisions away from us, but it can make recommendations as a second opinion, which is a positive effect of AI, especially when it comes to difficult decisions (Christen 2021).

Since the dawn of the scientific revolution in Europe around 1543, when modern sciences emerged and significant advancements in mathematics, physics, chemistry, and biology took

place, science became the path to discovering truth and learning facts to be the base for theories. There are many difficulties and challenges for science such as doubts about the efficiency of some scientific techniques because humans have inherently a certain degree of bias in performing scientific research (Briscoe and Fairbanks 2020). Additionally, scientists require a comprehensive understanding and experience in their field of expertise, a somewhat simpler task than it is today. They would need to read most of the published articles about a certain topic which was challenging enough (Briscoe and Fairbanks 2020). However, available scientific publications have radically increased, and the task has become almost impossible and overwhelming for humans.

Fortunately for researchers and scientists, databases exist for publications like Google Scholar and ScienceDirect to make access to scientific journals easy and quick. The challenge that is very hard for humans to meet is reading all about one specific subject. For instance, a search of ScienceDirect using the keyword "AI Security" gives over 24'000 results, which is growing with time. This area of research is relatively new, but it is growing daily. The same search on Google Scholar for the keyword "AI Security" returns over 2.5 million results which are impossible for us to go through. These difficulties with modern science research push scholars and industry to shift toward machine automation and AI to help simplify the huge load on scientists to analyze and process publications and data (Briscoe and Fairbanks 2020).

One of the essential foundations of U.S. national security is the preparedness and ability of its military forces. This preparedness is significant to avert and react to conflicts. The U.S. has for a long time enjoyed a superior position militarily that gives it the upper hand in most national conflicts (Briscoe and Fairbanks 2020). Nevertheless, this dominance is now being threatened by rising countries like China which is catching up very quickly and increasing its spending and investing in research and development.

Moreover, the U.S. national defense will likely strive to utilize the technologies developed by private sectors because they are strong financially and have the power to develop and produce semiconductors more than the government. China is under research in several related technologies like advanced microelectronics and space microchips. This approach will probably remain mainstream in the future (Briscoe and Fairbanks 2020).

The world's major powerful countries are spending money and dedicating resources to get ahead of their rivals. Much of the attention is on scientific AI, which will require a shift in the

shape of traditional government and a review of the national security strategy for the nations (Briscoe and Fairbanks 2020).

The increased information processing has led to new complexity and challenges to the current scientific processing. Therefore, a fundamental shift in technology development approaches connected strongly with national security is unavoidable, shall countries desire to preserve their international position (Briscoe and Fairbanks 2020). More investments and dependence on AI scientists will be the path for the near future. Nevertheless, ethics and values must be looked at by governments and policymakers when deploying fundamental changes in their systems.

The areas of influence for most modern advanced technologies are mostly used in optimizing logistics, spotting scams, composing music and art, researching, and delivering translations for texts. Smart machinery systems are improving our life and the quality of our services and products (World Economic Forum 2021).

The world is rapidly changing and becoming more effective, time efficient, and wealthier. However, today, people need to spend the vast majority of their time to grant an income to afford to live and sustain and provide for their families. Even now, this is insufficient if one wants to live a nice life and not be too worried economically. The talk is not about countries in the third world or countries in war and crisis. That is the case for advanced western countries where having one additional child can potentially collapse the family's economy. AI and its family have huge potential to change a situation like this for good. However, they only have the potential and do not make any pledges. The Japanese government does pledge to offer its people a bright future via all these new technology applications in the Super-smart Society (Cabinet Office 2018).

The only thing one could do is wish this would be a reality someday. Like that, humanity will have the chance to discover more meaning in non-labor endeavors. Things are more human-like, looking after our families, connecting with communities, and finding new ways to contribute to human society (World Economic Forum 2021). The magnificent contribution will add to the legacy of humanity in every domain, such as art, architecture, literature, entertainment, and much more. If the transition to the Smart Society is successful, future generations might look back someday and think how harsh life in 2020 was.

AI does not solve our basic problems

The Covid-19 pandemic and the consequently occurring scenarios drew attention to the use of AI and how radically it can create changes in our societies. After a few weeks of the pandemic, the crisis has had a global economic impact. Forecasters have repeatedly warned of the worsening future left behind by AI, which is a massive collapse in human employment (Christen 2021).

Obviously, in this case, it was not AI-controlled robots and software that replaced human labor, as many people were forbidden to work to slow the spread of the coronavirus (Christen 2021). For example, approximately 40% of jobs in Canada could be performed remotely, clearly with a big variance depending on the industry. However, for workers in professions that cannot be performed remotely, a large proportion of workers lost their jobs in the first two months of the corona peak between March and April 2020 (Gallacher and Hossain 2020).

AI stimulated change in the world of work that would never happen at such a pace. To the very least, the changes in society and, above all, in the labor market allowed people to draw attention to the potential disturbance of society through the extensive use of AI. AI resulted in an enormous shift in the income structure with extra social costs that forced the government to intervene massively (Christen 2021). The governmental intervention measures stopped a far worse catastrophe by decreasing business bankruptcies by approximately 50% and reducing the weaknesses of the corporates in the financial industry (Elenev et al. 2020). The important question here is, can the implications of AI trigger a such dramatic change in society in the future? The talk is about how people work and live and how their social life will be affected.

There has been, in recent years, a strong debate about AI (Gibney 2020; World Economic Forum 2021; Cath 2018; Cukurova et al. 2019; Brennen 2018; Greene et al. 2019; Risse 2019; Roberts et al. 2021; Ouchchy et al. 2020), which has intensified enormously after the Corona Pandemic. The ethical side of AI, the bias and the societal harm that can be caused, and many other significant problems need discussion.

3.1.8.2 Main Problems with AI

This subchapter is intended to shed some light on the most problematic issues with AI applications. The core issue here is that AI imports the problems from the developers and builds on them later. Unless problems during the designing stage are solved, AI algorithms will only carry the problems forward and not offer any tangible solution.

3.1.8.2.1 Racism and Bias

AI is supposed to help eliminate racism and not be a tool to deepen its societal troubles. Unfortunately, the practice shows different results, as seen before. Alphabet is one of the leaders in AI development and should carry the responsibility to give efforts to fight against racism. Though it revealed bias with its search engine Google when used to identify objects (World Economic Forum 2021), This issue has been well covered and worked around after complaints, but this is only the tip of the iceberg of the inherent problem. Search engines promote selective ideas, values, and identities that are intrinsically discriminatory and biased in favor of the groups that programmed them and the values of the corporations who established and funded these engines (Noble 2018). This issue is very serious because these search engines control what kind of information people learn. More dangerously, Google is not only telling the searchers the answers that Google wants to promote. It determines in the first place what is worth sharing! (Noble 2018). A similar phenomenon is observed on Twitter, Facebook, and largely on Netflix, where the massive dominance of these few media channels forces their values and beliefs on the global society to a large extent. The bottom line is that one should not omit that AI applications function as their programmer intended, and the solution for this issue should start there.

3.1.8.2.2 Media Effect – Business Effect – Education

It is now the time for media which has always been the strongest soft weapon, to force political and social change. It is time to use this soft power to promote ethical problems and create a public opinion that adapts ethical problems within AI applications. That will consequently create pressure groups that will gradually influence businesses and governments to regulate ethics and endorse ethical thinking in the AI designers' mentality.

If we do not change the mentality of the developers and those high-tech companies who pay their salaries, we cannot expect the algorithm to be socially neutral. Allowing businesses to run the way they are means consolidating the core social problems of bias and discrimination and

deepening them even worse in tomorrow's practices, where AI applications will replace people in decision-making.

Endorsing ethics in computer science studies will create a new generation of developers who will carry the challenge against digital bias and discrimination to a new level, which can negate a lot of the bad impact of technology on society.

Big technology companies like Google participate greatly in ethical research and promote ethics and societal values in their work (Gibney 2020). However, this does not mean that they are doing the world any favor! They have huge responsibilities toward society because of their positions. These research and practices to shine the image of high-tech companies should be their scapegoat, and they remain accountable for the damage, the harm they caused before, and the damage they will cause afterward. Otherwise, this will only be a part of political propaganda that pours oil on the fire of ethics-washing (Gibney 2020).

3.1.8.2.3 Non-ethical Problems - Are They Not Partly Ethical Too?

Unemployment is one of the biggest concerns for society in the medium and long run. Management on high levels in almost all corporates and all industries is preoccupied with job automation and digitalization. Technology's benefits justify the tendency toward adopting more digitalization within the corporation. It is not only about money-making or cost reduction. It is about survival in highly competitive environments and industries.

Fortunately, the creation of automated jobs necessitates creating intellectual and cognitive jobs that the machines, until now, cannot perform. So, to the very least, many new jobs will be created, but certainly not as many as deleted jobs. Jobs that people will perform will shift away from physical work towards more cognitive and intellectual jobs. These jobs will be dominant in the future instead of the physical work that dominated in the past.

Industries trucking in the United States provides jobs for millions of workers (World Economic Forum 2021). However, what will happen to these millions of jobs when self-driving vehicles arrive and mature? No matter how many new cognitive jobs will be created to preserve the functionality of self-driving vehicles, they will certainly not compensate for the lost jobs. Additionally, the United States will need to get rid of the existing vehicles, resulting in millions of tons of waste. Nevertheless, there remains an ethical advantage that one should not omit. Workers will be exposed to fewer accidents and work injuries (World Economic Forum 2021).

The example of trucks and truck drivers can apply to other industries like office workers and administrative employees. We are not downplaying the ease and fluidness of work and tasks that satisfy us as customers. It is about the need to find a solution or an alternative to the lost jobs and not overwhelm society with unemployment. The ethical side of the story is taking a job away from a person who supports his family and giving it to a machine to increase the wealth of rich corporations.

What ethical problems does AI carry?

The use of AI applications in human resources often results in copy-paste the dominant mentality of the company's approach. In many cases, this resulted in excluding older workers, foreigners, immigrants, and minorities (Gibney 2020).

Unequal distribution of the fortune generated by future machines is an ethical problem. The financial and economic system dominating has been built on reimbursement for contributions to the country's economy. That is regularly measured by hourly wage. Producing products and services in most businesses remains reliant on hourly labor. However, with AI being applied, most corporations are cutting down their human resources significantly to make more profit, and the profit will be shared with fewer people (World Economic Forum 2021). As a result, people who own their businesses will benefit largely by releasing as many employees as possible, and will add to their fortune. The rest of the workforce will be jobless and adding to the burden on the government and the unemployment fund.

Throughout the last 20 years, the technology industry has grown to be the most powerful in the world (Madrigal 2017). There are already signs of a wide wealth gap triggered by technology-based and start-up companies. When we look at the big three companies in Detroit, the largest automobile industrial city in the United States, and compare it to the big three companies in Silicon Valley in terms of revenue, we find that the Silicon Valley companies generate more money and hire fewer people. Table 3.4 shows the numbers for the year 2020. The figures are published by the respective companies online.

Table 3.4: Revenue and Employees for Largest US Companies in 2020

	General Motors Company (GM)	Fiat Chrysler Automobiles (FCAU)	Ford Motor Company (F)	Total
Revenue	122.5 B	127 B	155.9 B	405.4 B $
Employees	155 K	200 k	186 K	541 K
	Apple	**Alphabet**	**Facebook**	**Total**
Revenue	274 B	182 B	85 B	541 B $
Employees	137 K	135 K	58 K	330 K

What is noteworthy is the comparison of revenue and employee numbers in 1990 and today for the Detroit top 3. The revenue in 1990 was $250B with 1.2 M employees (Madrigal 2017). The automobile manufacturers managed almost to double their revenue and radically reduce the number of their workforce. Thanks to more advanced technologies and digitalization, the automobile industry and almost every industry improved its tool and increased their productivity. On the other coast of the United States, the top 3 Silicon Valley companies in 2014 generated $250B with many employees that reached 137K. Today, they doubled their revenue and expanded their operations to include around 2.5 times more working employees, which drives many to believe that employees in the automobile industry and any other industry that still depends a lot on human working forces should expect more disruption to their jobs. They should start worrying about their future shall the situation and the direction of automation not change or not consider the well-being of the human workers.

How machines influence our interaction with our environment

Machines are already affecting our behavior, how we interact with others, and how we behave in cyberspaces. AI bots are improving in terms of communicating with people and leading conversations. Chatbots are not a novel invention. They have existed for many decades. However, since 2016 the buzz about chatbots started to become more popular because of the advances in AI applications and the shift in social networking towards mobile phone messaging apps like Telegram and FB Messenger (Brandtzaeg and Følstad 2018).

The massive expansion in the mobile phone market during the last decade motivated the adaptation of more chatbots, so they became progressively more common to interact with customers (Smutny and Schreiberova 2020). Chatbots are being used for customer services and for promoting sales. If these bots are used in the right way for good purposes, they have a chance to push society toward more positive behavior. Chatbots have the potential to be effective in education and to be used in classrooms (Smutny and Schreiberova 2020). Though, they can also be used incorrectly and cause harmful consequences (World Economic Forum 2021).

Regardless of how chatbots are used, they indicate a shift in the interface between humans and technology and alter our dynamics and patterns of use (Brandtzaeg and Følstad 2018). That is a concern for society being subject to alteration in behavior even when it comes from one human to the other, all pushed and controlled by AI. The steering wheel for social life and regular habits is slipping away from people. AI applications are spreading into fields of application that no one ever expected a few decades ago. The question here is purely ethical. Should that be an accepted mark of the future society? Or should the international society and the local social organizations intervene to regulate the use of AI bots and further investigate its impacts on human society before it turns into a machine society?

3.1.8.2.4 Other AI Issues

Despite the huge leaps that AI has made in the past few years, it still makes many mistakes, even sometimes when performing a very simple task that requires very little human intellectual skill. The core of intelligence is acquired by the ability to learn new things; this is the case for humans and machines. AI applications usually go through training stages so they can learn to spot the desired actions and behave as they were intended to do. After completing the training stage, the application is tested to evaluate its ability to respond to environments. No matter how intensive and comprehensive the training is, the AI applications still run into different scenarios in real life, making fooling the applications easier in the sense that any human cannot be fooled (World Economic Forum 2021). It is much easier to fool AI applications. Computer scientists and AI researchers are attempting to resolve these weaknesses of neural networks (Heaven 2019).

Figure 3-3 (Vincent 2021) shows how an AI application sometimes identifies what it sees and how easily it can be manipulated. The test showed that the system could easily be fooled by

only using a handwritten label on the object that needs identification (Vincent 2021). There are countless examples of such system manipulation tricks that are very simple to apply and cannot deceive a real human.

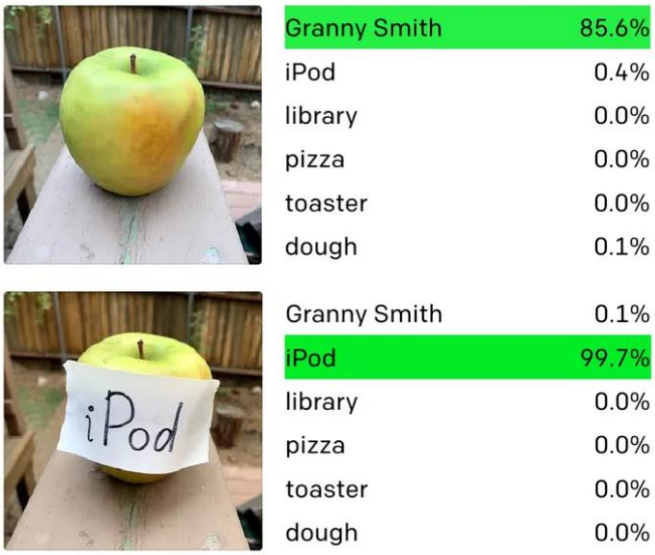


Figure 3-3: Manipulating AI

Therefore, it is possible to assume that we cannot yet totally rely on self-driving cars, for instance, as long as they can be relatively easily fooled when exposed to speed limit signs or other signs. All of that is apart from the real dilemma of the morality of this car (Awad et al. 2018). If we depend on AI to lead society into a new era of labor, security, and effectiveness, we have to make sure that the system operates as expected (World Economic Forum 2021) and that hackers manipulate it and cause any damage and malfunction.

3.1.8.3 Discussion and Observations

The progressive influence of AI is touching every single facet of the society we live in, no matter how trivial or critical that is. Critical domains like healthcare and humanitarian organizations and other social interaction and connections like dating have already been integrated with AI applications and robotics technologies such as ML. The main aim is to improve financial situations, enhance the welfare of all citizens, and elevate human rights levels (Cath 2018). Significant improvements to the praxis have been made in various domains, which hugely benefited from modern technologies.

Nevertheless, AI is prone to misuse, and its functionality can be unexpected sometimes and could consequently cause harm. The digital revolution is changing our perspectives about what

we have always regarded as values and as primacies. Therefore, monitoring and governing the technology tools are fundamental matters (Floridi 2018).

Common techniques are used to generate patterns from statistical analysis of existing data. Most AI applications apply these techniques as a learning method (Cath 2018). Controlling the possessors of the data would be the right focus point to govern AI uses. However, to be efficient, the regulations and the ethics of socially acceptable use of AI must be written and documented first. Then, the data owners and the techniques providers can be accountable for using their tools, and they should comply with regularities. Nevertheless, creating a governance body for AI applications is a huge challenge technically and socially (Cath 2018).

AI has increasingly strongly challenged basic human existing norms and human rights in the short, medium, and long terms. Short-term difficulties are present in how algorithms cause discrimination or enhance the existing discrimination to be more accurate. In the medium run, the challenges are apparent in the changing nature of jobs that humans perform for a living and the value of a human to society. While for the long-term challenges, future generations will have to live more closely to robots and machines and be more dependent on the intellectual abilities of the machines, which could be superior to humans (Risse 2019).

Another concern that AI raises is the influencing power which high-tech corporations practice over regulating AI. In some cases, they participate directly in writing the regulations. For instance, right after the Facebook and Cambridge Analytica scandal, Marc Zuckerberg was questioned before the US Senate Commerce and Judiciary Committee about the breaches for which Facebook was responsible. Ironically, the opinion of Zuckerberg was consulted in the same hearing session to rewrite the regulations according to what he thinks the law should be! (Cath 2018). Recently, the European Commission announced that it had assigned specialists to deliver guidance on the policy of AI for the European Commission itself. However, the participants in the former group include researchers from the scientific community, civil society organizations, and representatives from the top tech corporations (European Commission 2021). It is tough to trust the outcomes of the working group and not to question the credibility of the group without pointing out the conflict-of-interest issues as people from the AI companies are writing down the laws for their companies. Hence only 4 out of the 52 group members are from civil society, and 31 come from the industry (Cath 2018). The presence of civil society should be stronger when writing AI regulations, as society is largely

affected by the practices of high-tech corporations. The growth of business and the creation of wealth should not outweigh society's social matters and ethical values. A handful of companies should not possess so much power in the AI domain because the future of human rights, social justice, democracy, and ethics will all be reshaped with no serious governance from the real society, which is the main affected part of the coming transformations. Furthermore, future economic and political power will be in the hands of a few players (Nemitz 2018) and in favor of a few players.

The big technology companies have already launched some initiatives to protect and regulate ethical matters for AI, but only those suit their needs and visions. For example, Google has pledged to use AI to be socially beneficial and reinforce bias (Pichai 2018). That certainly adds up to ethical principles, but it is still far away from making a significant contribution to solving one serious social problem or answering one ethical question generated by the practices of high-tech companies via AI applications. Indeed, having ethical frameworks, defining technological interpretation of justice, and holding responsible parties accountable for their violation, in addition to forcing a level of transparency in the AI application programming, are necessary steps in the thousand-mile trip. It is crucial to tackle issues of strict laws and the internet's commercial and political advertisement business. The problems are not limited to scammers phishing everywhere we click on cyberspace. It is also about public manipulation and fake news spreading. The governance of big tech corporations will not be successful if these matters are not seriously included in the governance system.

AI was supposed to be an additional feature of the internet, but the momentum it is gaining promises that AI will soon dominate, just like the internet dominated our lives in the past few decades. The good potential of AI does not necessarily match the purposes it uses and develops. It is easily noticeable that only a few giant corporations control the development of AI. These are IBM, Yahoo, Alphabet, Facebook, Microsoft, Apple, and Amazon, in addition to some smaller influences (Nemitz 2018). Giant technological companies shape and control what we encounter in cyberspaces. They are almost the sole internet service providers. In addition to having incredibly profitable businesses as they see a constant rise in their value in the stock markets, they possess extremely political and economic power because they enjoy unequal access to lawmakers (Nemitz 2018) and influence governmental decisions (Cath 2018). Their influence reaches civil society, research, education, journalism, and science (Nemitz 2018).

Therefore, the superiority of these companies is true and not just from a technological perspective, but also regarding access to resources and public life.

There has not been such a powerful group of handfuls of corporations that managed to keep the services they sell away from regulations despite market dominance, public and lawmakers influence, and a distinctive concentration of control (Nemitz 2018). It is also critical not to underestimate the ambiguity of the use of patents and the secret agreements between the leading developers (Calvin and Leung 2020).

Despite the complexity of AI and almost the impossibility of seeing the entire picture in its specific deep details, it remains clear that AI is proving to be the current focus of the wishes and fears regularly brought up to information technology. AI will not free us from the basic problems that have always characterized our coexistence. It is not the development of AI itself but its interaction with us humans that is the anchor point for the positive use of this basic technology (Christen 2021). AI is like no other technology. The information processing techniques have inspired socially progressive and disruptive ideas in equal measure. The reason for this is probably that people increasingly tie their peculiarity to the ability to handle information. When machines intrude on this domain, it comes across as the ultimate slight and the most immediate form of loss of control.

However, the fear that humans will lose control and that in the future, only machines instead of humans will make decisions in important social processes is somehow exaggerated (Christen 2021). The reason is that people are building AI systems and coding algorithms. That is pushed by the desire to be enhanced by humans, but as humans with limited abilities, we need some further tools like AI (Ford 2018). Afterward, we use them according to our wishes as they can solve certain tasks better than we can. AI systems will not develop a conscious, and people will regularly test whether the system is still doing what it is supposed to and keeping under meaningful human control (Liao 2020). We need to be aware of the importance of preventing the use of AI from getting out of hand. That is not done by technology but rather by people's approach.

Whether people can accept a purely rational decision by an AI that can draw on enormous amounts of data is worth mentioning. Here we are not talking about complex questions that require data processing and complex mathematic problems. Will people see it fair when, in the future, only an AI was to determine whether to grant a loan according to rational criteria

(Christen 2021)? Amazon already used AI to fire workers from a fulfillment center. That puts the workers under much pressure to please an algorithm or risk their services being terminated (Hanly 2019). There have been protests, but Amazon did not provide details of the firing rate nor took any action towards a change. This decision-making approach will weaken the diversity of decisions and can be a serious problem for society if companies are left to their morals to rule their empires. We are not claiming that humans as managers do not make wrong decisions many times, but that is not necessarily catastrophic for the system as a whole (Christen 2021). How far will big corporations go? What else do they have in store for us as observing humans? The big corporations may be testing the limits of society's tolerance with their tools, pushing these limits further every day. AI tends to look objective. Nonetheless, it does not solve issues when dealing with human decision-making problems.

Some controversial applications and AI algorithms are how the police in Chicago deployed such a system to anticipate who would most likely take part in a public shooting, but the method they used was proven completely ineffective (Crawford and Calo 2016). A more worrying example of the misuse of AI is the famous case of Compas algorithm for the U.S. company Northpointe. Compas is one of many risk evaluation algorithms used in the United States to forecast geographic locations of violence and to decide the measures of regulatory oversight for suspicious people.

In 2016, the algorithm Compas categorized a man as high risk of recommitting an assault and sentenced him to spend six years in prison. The suspect appealed against the ruling because the algorithm's secretive nature violated his trial process. However, the Wisconsin Supreme Court ruled against the suspect (Yong 2018). Many experts said Compas is not better at forecasting offenses than random people (Yong 2018). However, this tool and many others in the same field are in use. The same algorithm is racist and biased against African people (Christen 2021). The cause of this bias is a consequence of the failure while programming by the developers, while the first example illustrates a misuse of the algorithm.

Researchers have shown that there is a basic problem behind the forecasting system: fairness or just. Just can be interpreted in different ways, and equally good reasons are integrated into algorithms. Deviating away from one form of just automatically results in other forms of just. Therefore, we cannot avoid the question of what kind of fairness is relevant in a given case (Christen 2021). This dilemma exposes a new issue that AI can create illusory objectivity that

does not relieve us of the responsibility to confront these basic questions (Christen 2021). That is not to argue that AI is an overrated technology regarding fears and desires. However, the central point remains that there must always be an interplay between humans and machines. Understanding and optimizing this interaction should be the goal of future research efforts (Christen 2021). We need to guarantee throughout the programming of AI algorithms, and when we think of the tasks of the AI applications, we need to guarantee that humans remain in control and that our future society does not lose out to machines.

The ethics of AI is gaining more importance and attention in international AI conferences. An important conference on AI in Montreal embraced human behavior in the reflection of AI, where issues like diversity, sexism, and inclusion were the center of focus (Nature 2018). More recently, in 2020, one of the most important ML conferences saw ethics merging as an area of debate and focus.

The emphasis on AI research progressively targets more ethical disputes encompassing AI technologies. Applications like face recognition and predictive policing have become more controversial as people and researchers question the ethical dimensions of these applications. They often negatively impact society and cause long-term harm to its structure (Gibney 2020).

The risen themes involve stopping biases in AI algorithms that mirror the current data bias models(Gibney 2020), especially since society is already susceptible and suffering discrimination problems. AI applications can worsen the situation if the bias and discrimination problems are not carefully addressed. The utilization of technology in useful ways that improve society's quality of life in areas like healthcare, education, and science has always been perceived positively. However, the debate about technology's influence, especially by ethicists, is another story.

Scholars and programmers now understand that they should implant ethics and values into the core design of research. There is an urge that scholars and programmers also comprehend the possible damages of digital inequality (Gibney 2020). The social implications of AI can be severe and potentially deepen existing problems like discrimination and racism. Additionally, the system must not cause harm and must protect from harm. Only structural change might not be the solution.

Is there a solution, or are we hopeless?

Fortunately, hope dies last. After examination, research, and thinking, a list of several measures can improve the situation gradually. The first suggestion is to encourage scientific journals to dedicate issues or part of their conferences to promoting ethical adaptation in AI. It is necessary to promote AI applications that aim directly to make an ethically positive impact on society and try to spot ethical violations within the society and handle the situation by using AI applications. Transparency can be a factor that helps foster ethical work environments. Programmers should be granted the right to know their end-product use (Gibney 2020). It should be regarded as a violation of their rights if their final products are to be used in an unethical way.

Implementations and Solutions

If we want to restore society's trust in technology again in the era of AI, as a first step: the impact of technology on society has to be seriously addressed and assessed by the policymakers to ensure that the public interest is the focus and the core aim of the regulators. Likewise, the impact of the new technologies on the developers of AI and the users of AI applications should be addressed and carefully viewed. The people should be aware of the potential change they can make; therefore, raising the level of awareness and sense of responsibility and accountability has to be aimed. Consequently, AI developers must be held accountable if they do not put ethical and social values and the benefit of society first. The top tech corporations and their developers must understand now that they have additional legal obligations to society. The penalties for breaches have to be severely damaging and are not only limited to financial penalties and fines. AI developers and engineers should not enjoy any protection from their corporations after they perform the tasks that they are assigned. However, this cannot be realistic and practical unless the authorities provide a clear code of ethics and detailed guidance, especially since there is always a place for articles' interpretation legally. Another necessary step would be empowering people who are the users and the affected by AI and representatives of society so they can introduce laws and adopt regulations, and have efficient monitoring over the applications of AI. In other words: making people the real sovereigns in the new era of AI. This might imply the creation of a governance body to perform the role of a union for technology practices for the welfare of humans.

Computer scientists are confident that AI will assist in reducing bias and battling racism, and solving many social problems. They argue that AI systems are certainly not less efficient than humans when conducting forecasts and determining certain decisions. However, many studies suggest that the same groups suffering in current human systems will continue or even suffer even more under AI systems. The reason behind that is the human factor that designs the AI algorithms, not the technology itself (Crawford and Calo 2016). Therefore, the starting point to fixing a broken system is to address the problem's root cause, which is the human. No mature ethics codes like "ethics of Artificial Intelligence" exist yet (Mittelstadt et al. 2016). Such guidelines for AI developers that focus on putting ethical practices while designing AI systems will be a leap forward in recruiting AI in favor of society.

Forming a strong front based on public opinion can significantly motivate the government to impose hard regulations for AI systems development. It is necessary to use the media and inform people about the ethical matters that accompany AI applications. Therefore, the debates about AI and ethics should be motivated to a greater extent. The media has a reasonably credible and useful focus in its coverage of ethical and social problems with AI (Ouchchy et al. 2020). The current discussion in the media concerning the ethics of AI is not concentrated on specific types of AI (Ouchchy et al. 2020). People are more interested in specific examples that attract attention, like when a self-driving car makes an accident. The approach to reach out to the people, raise their awareness, and gain their support is by promoting talks and debates about concrete examples of human privacy violations caused by AI and talking about the drops in employment rate due to applying more technologies and more robots replacing humans. The aim is not to ill-market AI technology but to capture the people's awareness and, consequently, the intention of politicians and governments to put serious efforts into writing down AI regulations that preserve the values and ethics of humans and do not ruin them. Merging the topics of society, ethics, and policies is not a simple task regarding the availability of information and the offered level of expertise from the speakers. Good knowledge of AI technology is also required. Otherwise, the content will be misleading or inaccurate. This suggestion involves expanding access to the right information to the public. It is in the shape of fact sheets and ethical value declarations on trustworthy and reliable internet platforms (Ouchchy et al. 2020) to assure that people are notified of the necessary facts.

AI reflection in Social Systems

Adapting AI broadly in various domains in our life will challenge the structure of society and the relationships between people within the society. For example, in healthcare, the relationship between doctors and patients is changing (Crawford and Calo 2016), and human contact is declining. The sense of safety for citizens is also changing while the police try to adapt algorithms to arrest suspects, assess risk zones, and intervene according to their computers. People will feel that they are not protected by humans like themselves but protected by machines that are prone to countless technical problems and failures. The public fear of computers taking over control grows bigger by the day. Many people fear that computers someday will outsmart people and control the world. The real problem is that computers are already controlling the world and are still stupid (Domingos 2015). Physicians already use AI systems to monitor diagnoses. Law companies are employing AI to consult their client and predict the probability of winning a law case. Banks use the same methods to assess the risk of giving loans to clients and make the decision (Crawford and Calo 2016). It is now very often seen how algorithms intervene in our lives, social affairs, business dealings, and even governmental decisions. AI is changing how we communicate and interact with the environment around us (Mittelstadt et al. 2016). There are gaps between the intended design of AI and how they function. If these gaps are left untreated, ethical effects seriously impact us as humans and the entire society (Mittelstadt et al. 2016). Several responding measures should be taken to protect society from such disturbance and limit some of the ethical impacts of AI systems.

The first is to assure compliance by corporations, so they hold on to the industry's best practices and fulfill their legal commitments (Crawford and Calo 2016). This step can create short-term improvements. Alphabet saw some responses to complaints about bias and racism in the Google search result. A partnership on AI research was formed by Google, Facebook, Amazon, IBM, and Microsoft to support social and ethical practices for the research of AI. However, Apple and Musk did not participate in this partnership (Hern 2016). We should not overestimate the efficiency of such measures as they are only superficial but necessary actions. The second measure is to promote values and ethics in designing AI systems. Computer scientists and technology companies should implement responsible innovation frameworks to recognize the values of their society in their coding when designing AI systems. Issues in focus

for the frameworks should include user privacy, ethical problems, social discrimination, and such matters. The values of potential users have to be afterward integrated into the design of the technology, whether it is a mobile phone application (Crawford and Calo 2016) or software for the auto-driving car (Awad et al. 2018). This measure can get extremely complex, especially for the products that will be used around the globe. That is because the values change from one country to another and form a culture in the other, even within the same country. The examples of cultural differences and society's favorite choices are countless. For instance, there is a significant difference in the interpretation of national security in the United States and the same in western Europe. The third measure will be conducting careful experiments on the adjusted AI application and testing their impacts on the application industry and the system's purpose on a societal scale and basically on the target groups that are often victims of unjust social practices.

Governments should not assume that AI will generate new jobs as quickly as it will delete them. Societies should not assume that new technologies will deliver wealth to everyone in society as technology did (Su 2018). It is not a secret in economics that technological advances generate wealth, but the ugly side of this truth is that not everyone in society can benefit from this wealth (Rotman 2013). On the contrary, many people will suffer from increased living costs and medical care. That is why we need to act immediately to be prepared for the future of jobs and employment in society in a manner that AI will help spread the generous advantages of automation out so that everybody can hope realistically for a future of enhanced leisure, fortune, prosperity and freedom (Su 2018).

3.1.9 Discussion and Conclusion

After exploring several risks and challenges for Society 5.0, the logical following question is: how can we overcome the challenges?

The solution to these problems is a crucial factor to consider. There are usually difficulties or hazards when society evolves toward a new form, such as Society 5.0. Early detection of these issues will enable much more focused and tangible action and makes it feasible to prevent hazards from developing into actual threats. The information learned here helps decision-makers from various fields make future judgments, much like opportunities do. The digital revolution impacted conventional sectors, making society more complicated.

Some drawbacks of a digital society, such as security dangers and data protection concerns, are now more readily evident (Fukuyama 2018). At the same time, there is a globally pervasive tendency toward utilizing digital technology to create new value and advance society (Bican and Brem 2020; Fukuyama 2018). It is impossible to ignore the path of digital transformation as it develops (Dufva and Dufva 2019). As a result, it is important to discuss and acknowledge these undesirable elements. Society 5.0 may address them and offer solutions to lessen the negative effects. Ministries and agencies, the legal system, technology such as policy, design, digital and technological ethics, human resources (Sima et al. 2020), and social acceptance of the numerous changes relating to the advent of Society 5.0 will all need to adapt as a result. The development of technologies and ecosystems for a future sustainable, human-centered, super-smart society for human well-being and security will be our worldwide task in the next decades, in which not only government but also industry and academia will have to play a major role (Fukuyama 2018; Aldabbas et al. 2020b).

Exploiting the potential of digitalization needs, among other things, to further organize the dialogue, especially in education. Grasping digitalization makes it feasible to analyze and debate digitality without the need for technical knowledge. For instance, bringing attention to people's ignorance of digitality and raising awareness through personal digitalization is possible. This understanding might also cause us to reconsider how we relate to the digital environment (Dufva and Dufva 2019). There should be a focus on how digital technology feels to teach our bodies to understand digitality, like how we train our ears to listen to specific noises. Nevertheless, it is important to remember the distinctions between the digital and physical worlds (Dufva and Dufva 2019) and that the platforms under the control of giant high-tech companies are the gate between these two worlds (Aldabbas et al. 2020b). The most suitable area for intervention to gain control is the platforms as Figure 3-4 shows (Aldabbas et al. 2020a; Aldabbas et al. 2020b). The needed intervention by the state starts with taking control over the platforms, which shifts the power from the hands of big tech corporations to the hand of the state. For more insight into the interaction between the real world and the virtual world, the reader is referred to the previous two references for further reading.

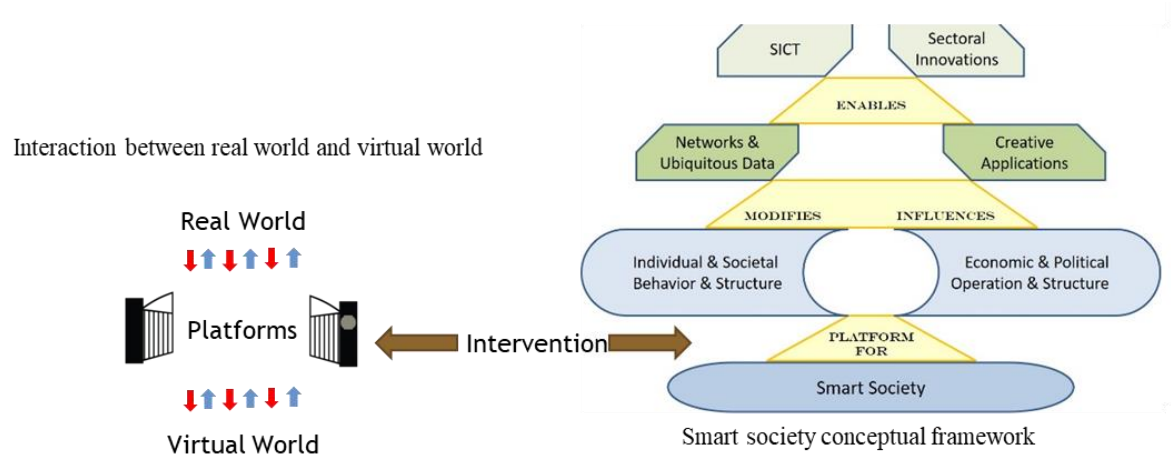


Figure 3-4: Intervention for Smart Society (Aldabbas et al. 2020a; Aldabbas et al. 2020b)

Chapter 3.1 provided a detailed answer to research question number 1:

> What are the most challenges that face Society 5.0 in the dawn of mass technology dependence? What security breaches accompany the technological revolution in the future?

The following Box 3-1 summarizes the answer:

Box 3-1 Answer to Research Question 1

Society 5.0 carries the same risks and challenges as the preceding information society (see chapter 2.1.4) but many of the existing challenges will take a modern and cyber shape. In other words, the problem will occur in cyberspaces in the cyber world as they do in the real world.

The future challenges are not limited to cyberbullying, blackmailing, online social exclusion, increased difficulties in securing communications, supply security, digital addiction, the negative impact of social media especially on the youth, and complex espionage practices. Ethics of the society will go through hard challenges, the labor market will change radically but slowly, more jobs will disappear than created. AI can easily carry the ill-intention of the programmers to society which will only enhance racism, discrimination, exclusion, and bias, and only complicate the solution. Advanced technologies like blockchain cannot automatically solve smart societies' problems. The issue is more profound than that.

This subchapter discussed some of the most important challenges for future Society 5.0. the future will bring unprecedented difficulties which will need a lot of preparation and more importantly a lot of adaptation. Of course, not all the problems are covered in this chapter as

it is impossible to cover everything. Nevertheless, some other issues will be discussed in a later stage of this dissertation, namely in the qualitative analysis chapter 3.2 because it is more relevant to be discussed when it is treated in depth. AI technology is addressed separately in this chapter due to its particularity and significance. The opinions of the experts in chapter 3.2 should be taken into consideration, and decision-makers in the concerned sectors should benefit from them.

3.2 Qualitative Analysis: Experts' Opinions on the Future

To envisage the future and to see whether there is a gap between the theoretical research and the forecast from one side, and the practical domain from the other side, a series of interviews were made with professional partners from different domains of expertise. The interviews cover issues for the future society such as the impact of digitalization on society, the future of the job market, the future education system, and more. Theory and practice sometimes differ depending on the research domain, the expertise level of the interviewed parties, and the intensity of the theoretical research[2].

3.2.1 Society Future and Digitalization

The first topic is the impact of digitalization on society and if the government should take any intervention measures, in which cases.

Expert A thinks that the push for digitalization that people have been talking about for a long time has finally happened, thanks to Corona. That is a good thing because digitization grows in schools, and homeschooling has become effective, a positive side effect of Corona. He adds that the phrase "digital wild west" reflects problems and fear in society, but it is not the task of the state to intervene. The responsibility lies with us, the people, regarding data protection, for example (this is a wrong approach that oversimplifies serious problems). However, according to him, the state should also set guidelines.

He adds that technologies such as AI, Big Data, and Blockchain will certainly bring changes to society, but it is hard to predict to what extent they will affect our lives. The changes that came because of technology in the past 20 years were extreme. However, this is not new to society as it was the case with all the big changes in the past, which will influence humanity. Future

[2] The interview questions were discussed well in advance with Prof. Dr. Stephanie Teufel (the first supervisor of this dissertation) and Dr. Bernd Teufel. Janick Spycher, a former student, conducted all the interviews within the framework of his master's thesis at the iimt. The interviews took place online using the platforms MS Teams and Zoom.
For data protection and privacy, the names and the positions of the interview partners will be anonymous. The transcripts of the interviews are not provided here either. However, all this content is available in (Spycher, 2021). See appendix 7.1 for further insight.
The answers of all experts for each topic will be grouped and presented. The findings will be compared to the theoretical research and the forecasting outcome.

changes will affect traveling, working, and so on. There will be positive and negative changes in society. Life will be easier for those who can use these technologies. Others will be overwhelmed with technology and might get lost.

On the other hand, the basic values of humanity could be lost as a result. The term better future depends on the context of "better". Compared to the former generations, issues such as contentment and happiness are defined differently. For people who have grown up less with this broad and fast digitalization, it will certainly become increasingly difficult to keep up in the future, which could lead to the fact that these people will lead a "worse" life, "from their point of view" due to the change in the future. These people should be helped.

Expert B has a similar impact on the matter. However, he prefers, instead of trying to answer the question of how future technologies will change our society, to ask ourselves what we have to deal with to maintain high-value creation and high wage levels in Switzerland, to have a stable currency as well as to remain a peaceful place. We have to deal with the fact that algorithms are becoming more important and have been for at least 30 years. Are software and algorithms something that will become more important? These questions will occupy us for the next 20 to 40 years, and at the moment, we can observe that too little has been done to consider this fact. Too little is made for education, and the structural transformation of companies is proceeding rather slowly. Investment activity in Switzerland in digital business models is rather modest. On the other hand, a lot has been done, and people have always financed important universities and ensured they have a good reputation worldwide.

Expert B adds that the basic laws to protect us and our data are in place. What is currently being done with the GDPR is wrong because there is no need for the state to regulate how specifically to handle data, but the laws regulate how to handle data. Additional regulations will not lead to the protection of data or local companies; rather, new barriers will be created that make participation in the digital economy more difficult. (Perhaps Expert B is not completely aware of the real threat of data mishandling).

Expert C thinks that society is already changing today and will continue to do so because digitization and AI methods are very broadly applicable and will therefore become more prevalent in our everyday lives. He adds that digitalization is like a tool that can be used for good and evil. For example, Google's Natural Language Processing tool is like a cannon, like a tank, which can be used for defense and destruction. There will be a need for new regulations

in the future in this context when it comes to the role of the state. Politics has the task of eliminating grievances, but at the same time, it also has to support entrepreneurial thinking.

Expert D says that there are three areas where technology will affect society: computing power, connectivity, and cognition. These three areas have different main effects, direct and indirect. The direct effects are the whole process of interaction and transaction. There will certainly be fundamental changes. The time in the office is also over. People will be much more flexible and less location-based. However, how will society deal with such a change? Society will slow down and channel this change somewhat, which is good. However, solutions will certainly be found within society.

On the state's role, Expert D thinks that the state does not need to do either more or less. It needs to do it right. One problem with all new developments is that our system is a bit slow, so passing regulations is always difficult and lags behind. He adds that in terms of implementing the aspects of Society 5.0, there are always two different approaches to transformations, either bottom-up or top-down. The Swiss system is bottom-up. Compared to other countries, the Swiss government does not have clear strategies and does so consciously. Now the question arises of which method is better. The top-down method is certainly faster, while the bottom-up method requires more time and resources. However, with the bottom-up method, the error rate is smaller. The Swiss approach is not bad, but a mixture of these two methods should apply.

3.2.2 Changes in the Work Environment

The real estate market will have a huge upheaval. Expert A believes that consulting firms will not be affected too much in terms of changing working environments as many firms do not need big offices and huge spaces to work. There are already many vacant offices. Google plans to stick more to the home office and downsize the office spaces. Big corporations like Swisscom and Post might consider the same approach as well. There will be people who will enjoy working at home. Others, however, will probably become lonely because social contact will be lost to a certain extent. One cannot make up for that with a digital coffee break. Face-to-face interaction will remain important in the future, but it is still a huge opportunity for us as a society.

Digitization and automation will lead to a rationalization of jobs in certain industries. On the other hand, however, it will certainly also create many new jobs. So, one could call it a shift or a relocation. Future employment will be easier for younger people. Industry 4.0 has been a topic for a long time, but unemployment has not increased. People have probably adapted to their respective situations.

In the opinion of Expert B, when new tools come to hand, the old ones are not forced to be abolished. However, the old tools will have less importance. Due to the lockdown, people who previously could not do anything with the home office can now recognize its advantages. Concerning teleworking, the concept of the office has been changing for several years. Individual offices are less used. There are more workspaces where people can meet and interact with each other because the work to be done in the office is work where the considerations of several people are necessary. However, teleworking will be used more for work where interaction is unnecessary. It will gain greater acceptance by supervisors.

The number of people who "fall out of the system" because they cannot keep up with the change in technologies is not as small as one might think. To counteract this problem, there is a need to strengthen people's ability to work through job profiles promising for the future through education and training and on-the-job training. Here we are dealing with technical issues, but there is another aspect, namely that of health. One has to be physically and mentally healthy. The Covid-19 pandemic would have been the perfect time to introduce an unconditional basic income.

Expert C believes that jobs will disappear as a result of new technologies. These changes will happen, whether it is good or bad. The urging question is: what happens to the people who lose their jobs or are intellectually unable to cope with this digitalization? No answer has yet been available to this question. The solution is not to ban technologies but to discuss them openly and find different solutions. If one wants to introduce the basic income, the proposal at that time must be adapted, for example, with the adjustment of the social work, from the different workers one becomes. The experts in this field are facing challenges in developing a system suitable for the majority and the masses.

According to Expert D, when new technologies arrive, appropriate skills will be necessary to deal with them. There will certainly be negative consequences during the transition period in this context. There will be a change in the labor market, so certain jobs will be lost while others

will be created. Fortunately, there are functioning social systems in Europe that prevent these people from ending up on the street. The social systems have to be adapted accordingly to be able to cope with these future challenges.

In the context of job losses, the most efficient way would be to introduce a basic income. One can only delay progress with such measures but not stop it. Civil rights must be translated into the new age and adapted accordingly. One must look back to the past, how many similar problems were solved, and orient oneself on these solutions. There is a need for an unconditional basic income. As a result, people can decide what they want to do regarding their profession because they are secured to a certain degree. Moreover, various insurance would be eliminated and the relationship between the state and the citizen would become stronger.

3.2.3 Future of Education

Expert A says that the introduction and the implementation of homeschooling is a good thing, but currently, there is no standardization in distance learning as some schools have gone under and could not be up to the challenge. Some teachers were not skilled enough to educate students distantly, and the burden was on the shoulders of the parents, but the situation will be improved in the future.

As per Expert B, on the one hand, there is the manufacturer's point of view where there are people who write algorithms or produce software, and on the other hand, there are software users. There is a boundary merging where the developer's role ends, and the user's role begins. That is becoming more like a fluid. More semi-finished products are available, with which the end user can put together his processes. So, there will no longer be just programmers and users, but a mixture of both. To do this, the user needs a certain competence, and the most suitable source for these competencies should be acquired from the education system.

Expert C says that two areas of action are needed. First, IT specialists are promoted more strongly, i.e., in a narrower sense, digitization specialists. Investments should be made in computer science apprenticeships or computer science universities of applied sciences and training courses. Secondly, digital skills are considered future skills. So, for example, all students from all fields of study should have an idea of programming. For this purpose, the basic course

"Programming" has been offered since the beginning of the year. However, such courses should not only be offered at the university level but also all levels of education. When it comes to implementation, one should consider whether the students can handle the material and whether the teachers can. There are various ongoing projects for this, so the adjustments in education, in this context, are on a good path.

For universities, digitalization is a great opportunity from which more could perhaps be made. The Corona crisis shows very well that it was important to introduce Ilias (an education platform used at the University of Bern). The mobile app, which is currently in progress, will certainly have the potential to achieve benefits for students. Furthermore, more needs to be invested in digital and future skills.

Expert D thinks the university system is facing a big change for several reasons. Many universities are still set up as they were in the past in connection with their structures. Corresponding changes in the structures are difficult to implement. However, they will be necessary sooner or later and will be implemented accordingly.

3.2.4 Technology Ban

Expert A says that from a business point of view, it is not desirable for the state to intervene too much in the businesses and the technology in use. Conditions and regulations will weaken the competitive position of Switzerland. Concerning the example that Japan uses robots to care for people, there is also a shortage of skilled workers in the nursing sector here in Switzerland, but there is also a fear of losing the human touch in such developments. It is unrealistic to achieve enough acceptance for using robots in older people's homes or hospitals in Switzerland. Because of the ethical component in this question, it is certainly difficult to envisage the state as a regulator here. A reasonable approach in applying controversial technology is holding the user accountable, for instance, with the example of autonomous cars. It would be too high a risk for the manufacturer or programmer to assume liability. To be so sure that the own product does not make any mistakes is almost impossible for a manufacturer.

Expert C believes that laws to ban technologies should not happen and that politics always has a role in reacting, i.e., in the sense that something should only be banned when it happens. Otherwise, innovation would be prevented.

Expert B opposes technology banning and thinks it is rather dangerous, so if one technology is banned to protect an existing structure, then this structure will be preserved, and change will come much later. Therefore, releasing technologies is the better way because it makes changes grow more slowly and not all at once very quickly. However, there are technologies, for example, that can be called war material, which must be banned or regulated. What is needed is not necessarily new laws but controls and appropriate monitoring of the laws already in place.

To prevent an accident, self-driving cars must decide whether to endanger the driver or a third person. A human being should always make such a decision.

3.2.5 Summary of the Interviews

This sub-chapter summarizes the most important points and insights discussed by the experts. Some opinions showed conflict with the finding in the theoretical research. These points were mentioned in the interview presentation parts. Not all experts come from the same background. Therefore, the summary notes are being taken accordingly. One last remark on the interviews: the Covid-19 pandemic might have influenced the experts' opinions. That means that if the interviews took place before the pandemic breakout or after the dangerous waves faded away, the expressed opinions could be somewhat different on certain matters.

Table 3.5 shows the most important notes and takeaways from the interviews.

Table 3.5: Interviews Summary

Domain	Trends of opinions
Future of society and digitalization	The covid-19 pandemic pushed digitalization forward in society. This means that society is already changing. The state will need to set guidelines. Society might witness new divisions. Swiss policymakers should be more agile and integrate a top-down approach into the legislation.
Work environment	The real estate market will mostly be challenged. Big corporations will alter their systems to reflect a better life-work balance for employees, but other social problems will emerge. Workers will need to strengthen their abilities to not fall out of the new system, but many jobs will disappear.
Future of education	Universities worldwide face big challenges, and old mentalities must change or be ignored to advance. The absence of systematic standardization in distance learning is hurting homeschooling. Digital competencies are gaining more importance in universities, and the adjustments in the education systems are on the right path.
Technology ban	Banning technology will weaken competitiveness in Switzerland and hinder innovations. Appropriate control over the use of technology is needed instead.
Recommendations	It is time for the state to introduce a basic unconditional income. Boost the education system towards more digitalization and properly educate the teaching forces.

This subchapter provides the first part of the answer to research question number 2:

> How will the future society impact the lives of individuals? How will technology affect various aspects of life?

The summary of the answer is in Box 3-2:

Box 3-2: Answer to Research Question 2 (part 1)

Digitalization will speed up and people will have to cope with it and increase their IT skills. Otherwise, there is a huge risk of being cut off from society as new social divisions might appear and the living standards for those people will drop. Many jobs will disappear and employees will suffer to keep up with their tasks which creates big social problems. Future education requires more digital skills but the education system is not advancing enough in Switzerland which affects the position of Switzerland globally and will have an impact on the economy locally. Ethical problems started emerging due to automation and so far, the state is not taking any measures which risk complicating some existing social problems. Poverty will increase as people will not afford to maintain their living standards which call for reconsidering basic unconditional income and considering financing that via taxing robots and machines.

Next chapter 3.3 continues the security and challenges analysis for the future using quantitative approach.

3.3 Quantitative Analysis: Forecasting Key Figures for the Future Society

The forecast in this work aims to shed some light on the effects of the progressive advancement of technology on Society 5.0 for some selected attributes of civic and private life. The whole forecast attempts to predict in which direction our society will evolve in the near and further future. How will this change impact our lives? Moreover, will that be in favor of us as humans? Or will the new evolution favor the big corporations and create value for a certain layer of people only?

A short introductory part is necessary to serve the purpose of the forecast in a manner that avoids confusion and answers the questions raised.

3.3.1 Introduction to the Aim and the Approach of the Forecasting

Chapter approach and bullet points:

1. The only thing that moves predictably and staidly is time. Therefore, all the variables in this chapter will be treated as time series variables.
2. Looking at where we were a few decades ago and where we are now, more digitalization is applied in society. What is a digitalized society in the context of this research? This question needs an answer, or else much confusion will be around.
3. The conducted research showed that there are two types of variables, each of which has its characteristics in terms of cause and effect perspective:
    a. The first type is the cause, which motivators advanced digitalized society, namely investments in Gross Capital Formation (GCF), and Investments in ICT. These two factors push society toward digitalization. The two variables will be forecasted because they play the role of motivators for society. An explanation will follow (see Figure 3-6). This group can be seen partly as independent variables that affect and lead society to its future.
    b. The second type is the effect. It composes 20 identified variables that reflect the most important figures in our life. This group tends partly to be dependent variables affected by the first group. This group is also the subject of the forecast.

c. However, it is too strong of a statement to treat the two groups as dependent and independent because of several reasons:
    i. The economy is far more complex than only these variables.
    ii. Considering ICT and GCF as independent variables is an oversimplification of the problem and not an accurate economic assumption. For example, GDP numbers are enormous compared to the two independent variables. In addition to the potential overlapping between components in the two categories, some investments in ICT can appear in the total figure of GDP. Therefore, treating GDP as a product or a function of only the two variables is not logical.
    iii. There is no tangible benefit or advantage of carrying on such analysis (dependent/independent) than statistically treating all the variables as independent time series.
    iv. The level of complexity increases massively in the case of using a suitable advanced method such as cointegration analysis that treats the variables as dependent and independent. Additionally, economically speaking, it is too difficult to justify assumptions such as "GDP is a function of ICT". The other way around makes more sense! Nevertheless, it is also not true.

4. The distinction between the two groups is just for the sake of logical thinking and a better understanding of the factors that affect society and their role.

3.3.1.1 Defining the Factors that Shape a Smart Society

Smart society is an advanced society with digital nature, as it transforms society for the better by utilizing digitization and connection across platforms and throughout society (Holroyd 2022). Identifying the meaning of an advanced digitalized society is very important for the scope of this part of the research. There is a need to know what characteristics the digital society has, so that related variables can be identified. When discussing the indications that make a society advanced and digitized, it is essential to consider the description of the European Commission (European Commission 2020). The categories are presented in Figure 3-5 based on (European Commission 2020). There are five main categories. Namely:

connectivity, human capital, use of the internet, integration of digital technology, and digital public service.

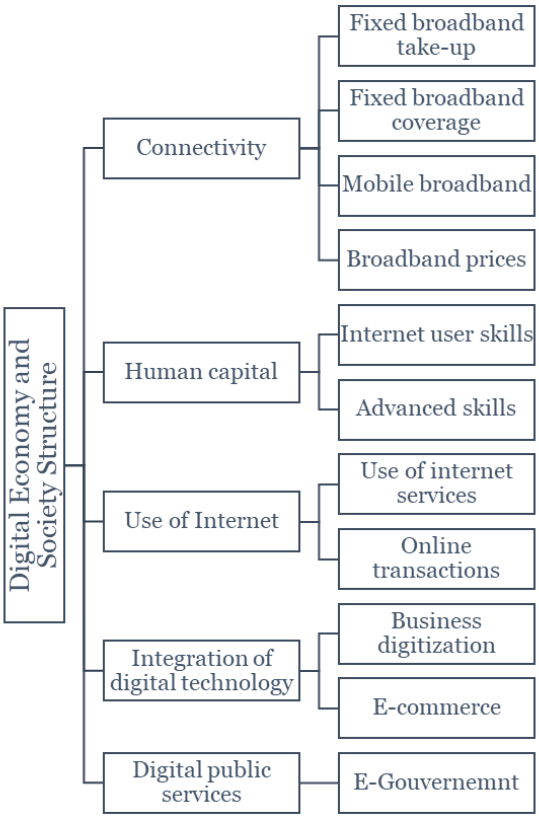


Figure 3-5: Structure of digital economy and society (European Commission 2020)

Now, while looking at all these five categories and their sub-categories and thinking of them hypothetically as outcomes of certain inputs, the intuitive question comes to mind: what are these inputs?

Fortunately, the answer to this small question is found after much research. These five indicators can be considered as consequences of investments in ICT, and investments in GCF. Other indicators might also exist, but for the time being these two input variables sufficiently represent advancement and digitalization in society. This finding is presented in Figure 3-6. The explanation and justification follow directly.

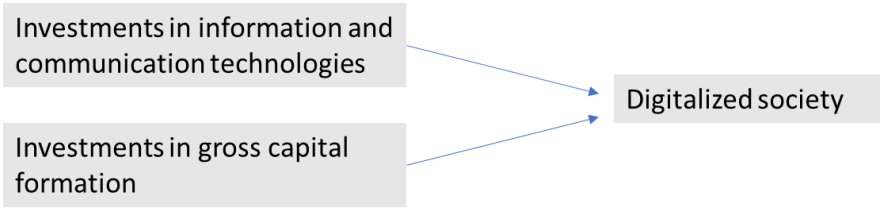


Figure 3-6: Inputs for Digitalized Society

The first two indicators/categories of digitalized society, connectivity, and human capital are sufficiently and suitably covered within the GCF. That implies that the more the country invests in its GCF, the more digitized and advanced its society becomes. The rest of the factors are included in the notion of ICT investment. Hence that there might be some interconnectivity between these factors and their cause. For instance, promoting internet usage is a mixture of investment in ICT and investment in human capital equally and through different channels such as school and work.

The first independent variable will be the investments in ICT, and the second independent variable to represent digitalization and advances in society is the investment in GCF. The latter is formerly known as gross domestic investment and consists of outlays on additions to the fixed assets of the economy plus net changes in the level of inventories. Fixed assets include land improvements (fences, ditches, drains, and so on); plant, machinery, and equipment purchase; and the construction of roads, railways, and the like, including schools, offices, hospitals, private residential dwellings, and commercial and industrial buildings. Inventories are stocks of goods held by firms to meet temporary or unexpected fluctuations in production or sales and "work in progress.", net acquisitions of valuables are also considered capital formation. Data are in the current local currency (World Bank 2021c).

For consistency reasons, all the figures are represented in the current currency. This means the value of the currency for that year. It can sometimes be referred to as nominal currency. The other alternative that is equally published, especially by the World Bank, is the constant currency which presents the data for each year in the value of a certain base year. This method takes inflation and other economic notions into consideration.

3.3.1.2 Challenges to Obtain Useful Data for the Forecast

The first challenge to run a representative forecast for the future strongly correlated to technological advancement lies in the scarcity of data that can be used. The available data published by the Federal Statistical Office (FSO) offers limited but useful value. For instance, the published figures about the years before 2000 are strongly misguiding due to the huge leap that happened in Switzerland and the entire world. This means that there is a restriction on the range of useful data, which is only from the year 2000 through the year 2021.

The second challenge is that the available numbers do not cover entirely all the areas that are wished to be forecasted. Additionally, some data for some years are unavailable, which makes the forecast's accuracy slightly weaker.

Third and foremost, numbers cannot reflect a society precisely. In this case, measuring technology advancement and reflecting it in numbers for the forecast is essential. Otherwise, there will be no forecast. It is not enough to have numbers that describe the current situation, as the aim is to observe the transitional effects on society for a certain period. That means that the available data can only be useful if they are available from the year 2000 through 2021. The only useful figure that represents a certain limit the technology advancement in society is the investments in information and communication technologies and the GCF investment. Only these two variables are the engine that moves society forward into digitalization. Figure 3-7 explains the concept of the forecast purpose. The forecast aims to study the inputs' impact and how they interact with the process to predict the outputs.

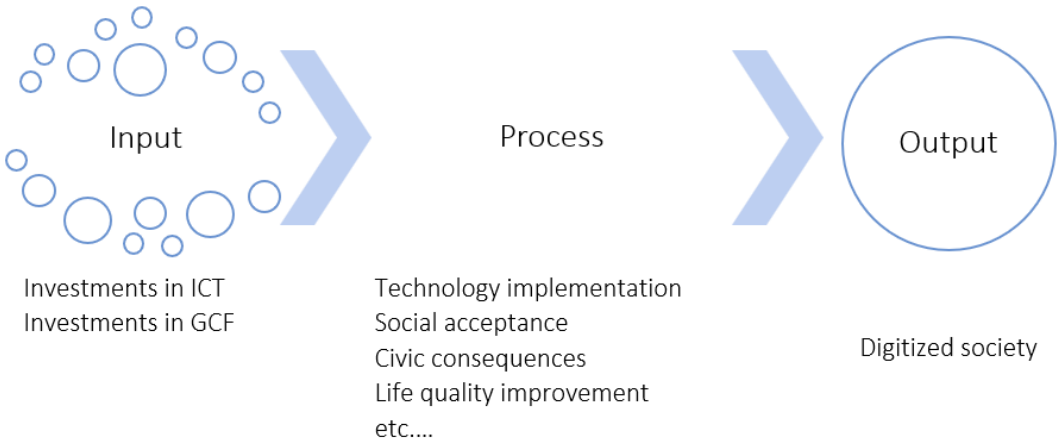


Figure 3-7: Concept of the Forecast

Fortunately, these two key figures for the inputs are available for the time range that is needed and offer an indication of the technology adaptation level in the society in Switzerland. However, the problem is not solved completely yet! and here is why:

Measuring technology and technology application in societies is a difficult matter as numerous indicators show the implementation of technology in the various domains of life. The real deal here is knowing exactly the purpose of posing the question and understanding why evaluating technology applications is necessary. Intuitionally, the public investments in ICT figures indicate a certain limit: the advancement of society and technology. However, the figures for the money

invested represent only the money spent and not the return on these investments. Not every investment is profitable, and not every project is successful. Besides, the domains of investments can vary significantly, and the interpretation of their contribution to society's advancement will also vary. For example, replacing an outdated healthcare system based on basic pen and paper with a new digital system indicates that the state is taking a digital approach and implementing technology successfully. However, the real improvement to society is somehow limited to better communication and flow of information, and better data storage. This does not mean that society and people have gone digital. Therefore, this figure has not provided many indications of the advancement of technology adaptation. It rather has more meaning in the holistic pool of investment that touches countless aspects of life.

The second key figure is the GCF. It comprises a vast range of investments in infrastructure, hospitals, education systems, and human building. It means there is no way to know where each Franc invested will go and if it will serve the purpose of digitalization. Nevertheless, cumulatively GCF boosts society and technology.

Regrettably, not much literature has addressed objectively measuring technology adaptation in a society coupled with social progress. Some tend to measure technology adoption by the proportion of farmers who use modern technology and/or the percentage of the land area where this technology can be applied. Again, this will depend on the driver and the motivation to measure technology adoption and its context. For instance, if one is assessing rural public policy, then this figure is a very good indicator. However, other elements must be considered, like the percentage of farmers in that area, accessibility to technology, and the number of animals on farms that are under technology. The point is that there are so many indicators for technology adoption, and these indicators can give a brief image if they are put together and added to one another.

In a different domain like the retail market, the proportion of customers who chose the online shop for their purchases over the physical store reveals the level of technology adoption and acceptance. The same thing applies to banks and the money transfer market. The higher the percentage of customers opting for online activities, the higher the advancement of society in terms of technology is. Also, the annual numbers of electric car sales show the trends for future mass dependent on technology. The increasing number of social media users also points in the same direction. The usage of the services of the e-government implies the acceptance of

technology and especially the trust in society. These previous examples show the variance in technology advancement assessments and societal implementation. Unfortunately, it is very complex to comprehensively cover every single factor to measure and compare societies and derive solid data that can be used for further analysis and research on a nationwide level.

All indicators can be useful measures to indicate technology adoption, but the intended aim of the study determines the important choice. Thus far, the official numbers of investments in information and communication systems in Switzerland are the only solid data that directly engage in forecasting the future of society. Hence, some limitations and matters must be considered to avoid misreading the values. For instance, not every investment is a successful investment, not all the technology that will be invented will be applied, and not all the technology applied will be accepted and used in society. Nevertheless, the investments in ICT do represent a robust indication of technology adoption in an advanced society like Switzerland.

The most important thing is that two independent variables are defined as useful for the forecast. These are investments in ICT and investments in GCF. The main question will be finding suitable forecasting models and the validation of these models by appropriate tests. Additionally, several dependent variables will be identified within the field of research. These will be discussed as well in detail next.

3.3.2 Selected Areas for the Forecast

The problem concerning the difficulty of representing society in numbers implies a limited area of focus and, therefore, a small number of variables that can be measured. Nevertheless, despite this narrow range of choices, important attributes strongly concerning society are forecasted. Some areas have several attributes that can be forecasted. Therefore, some areas will have more variables than others. The areas of focus and the variables are demonstrated adequately in Table 3.6.

Table 3.6: Areas of Forecast

Area of focus	Variables for the forecast
Investment and incentive	Investments in ICT
	Investments in GCF
National level	Gross Domestic Product (GDP) in USD
	Gross National Income (GNI) per capita in USD
	Inflation rate
Healthcare	Healthcare Costs in millions of CHF Workers in the healthcare sector
ICT services import/export	ICT goods imports (% total goods imports)
	ICT service exports
	Medium and high-tech exports (% manufactured exports)
Internal businesses	Number of new businesses registered
	Number of SMEs
Labor market	Labor Force Participation in the Labor market in full-time equivalents Employment in the retail sector for males and females
Unemployment	Unemployment, total (% of the total labor force)
	Unemployment, male (% of the male labor force)
	Unemployment, female (% of the female labor force)
	Unemployment with basic education (% of the total labor force with basic education)
	Unemployment with advanced education (% of the total labor force with advanced education)

3.3.2.1 General Comments on the Data and the Forecast Variables

Most data are derived from the FSO and the World Bank. The sources will be noted accordingly in the datasets for forecasting. Hence, some data is available quarterly, and for simplicity reasons, the last quarter's data is considered. There is no significant variance or further

implication observed. Hence, some elements of the following discussion on the selected forecast areas necessitate more insight than others.

One final remark, as mentioned earlier, the values that will be presented are the values in the current local currency.

3.3.2.1.1 National Level Figures

Gross Domestic Product (GDP) is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products (World Bank 2021a).

Gross National Income (GNI) per capita is the gross national income, converted to U.S. dollars using the World Bank Atlas method, divided by the midyear population (World Bank 2021b)

Inflation defines the adjustment in the price of a specific basket of goods over a certain period. The Consumer Price Index (CPI) measures the price changes monthly. Inflation is normally defined as the change in the yearly average of the CPI (FSO 2022b). A historic overview of the inflation rate is presented in Figure 3-8 (FSO 2021b).

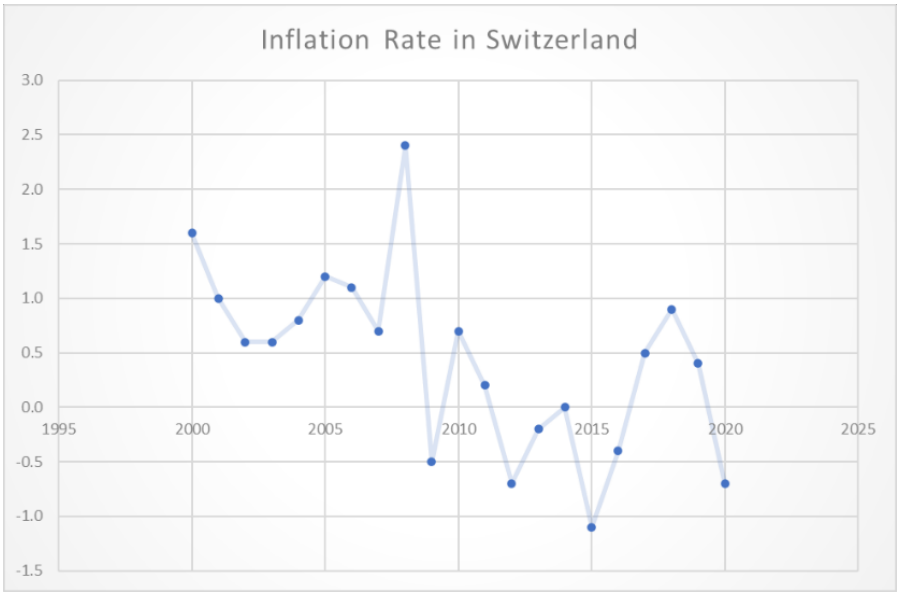


Figure 3-8: Inflation Rate in Switzerland (FSO 2021b)

The official CPI in Switzerland for the year 2021 contains the following elements as per FSO (FSO 2022a): food and non-alcoholic beverages, alcoholic beverages and tobacco, clothing and footwear, housing and energy, household goods and services, healthcare, transport, communications, recreation, and culture, education, restaurants and hotels, other goods, and services. The respective weights are presented in Figure 3-9 (FSO 2022a). One should keep in

mind that the Russian invasion of Ukraine has an impact on inflation in the Switzerland and entire of Europe.

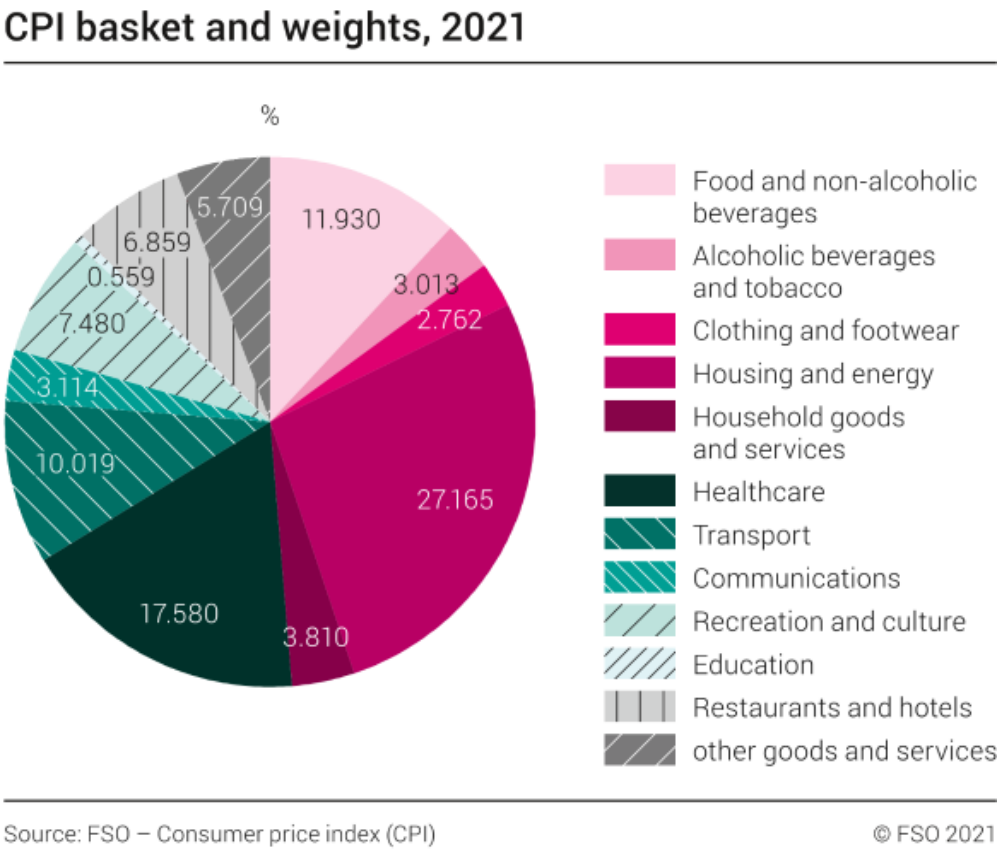


Figure 3-9: CPI Basket and Weights (FSO 2022a)

The forecast aims to examine the relationship between the abovementioned figures representing the country holistically and the technological advancement in society. The three dependent variables will be tested against the sole dependent variable, i.e. investment in ICT.

3.3.2.1.2 Healthcare Costs

The forecast assesses the implications of technology adaptation on healthcare costs. The aim is to determine if the costs of the healthcare system in Switzerland will increase or decrease in the future with future technological innovations and investments in ICT.

Some other interesting factors could be considered regarding the healthcare system, such as differences in the acceptance of technological support in hospitals and medical praxis by both patients and workers, the availability of skilled workers in healthcare occupations, and the job market status in this domain. One should not omit the new condition due to the Covid-19 pandemic starting in late 2019. However, apart from the unavailability of enough input data, investigating all the details of the healthcare system will require additional work that does not

necessarily serve this dissertation's purpose. Therefore, only one dependent variable, "Healthcare cost" will be examined in the forecast.

3.3.2.1.3 ICT Services

This part concerns the impact of technology on the ICT market in Switzerland. Three variables are defined: the change in ICT imported goods as a percentage of total imported goods, the change in ICT services exported, and the change in the proportion of medium and high-tech exports.

3.3.2.1.4 Internal Businesses

The forecast covers the situation of the businesses within Switzerland in two attributes: the annual number of newly registered businesses and the annual number of registered SMEs. The importance of SMEs to the local economy comes from the fact that SMEs add up to over 99% of the firms in all industries. Moreover, SMEs generally generate over 66% of the jobs in Switzerland(FSO 2021c). It is important to note that according to the statistics of FSO, any business with less than 250 persons is considered an SME.

3.3.2.1.5 Labor Market

The forecast focuses here on the labor forces actively participating in the job market and its correlation with ICT investments as society approaches Society 5.0. The lone dependent variable under study is the labor force participation in the labor market in full-time equivalents.

3.3.2.1.6 Unemployment

The definition of unemployment must be discussed to avoid confusion and clarify the matter. Unemployment is used in this forecast according to the definition of the International Labour Organization ILO. According to the ILO, unemployed persons are persons aged 15-74 years of age, who were not gainfully employed during the reference week, have actively sought work during the previous four weeks, and would be available to take up employment (FSO 2021a). The published data by the FSO on unemployment takes several forms and two models. The national model and the ILO model. There is almost no difference in the unemployment rate between the national and ILO model. The data used for the forecast is the ILO-modeled data sets.

The unemployment data covers all the residents of Switzerland aside from their nationality. The data is more representative of society and avoids discrimination when speaking about

society. However, it is important to keep in mind that the unemployment rates are significantly higher for foreigners in Switzerland than the Swiss nationals, according to the FOS, as can be seen in Figure 3-10 (FSO 2021a).

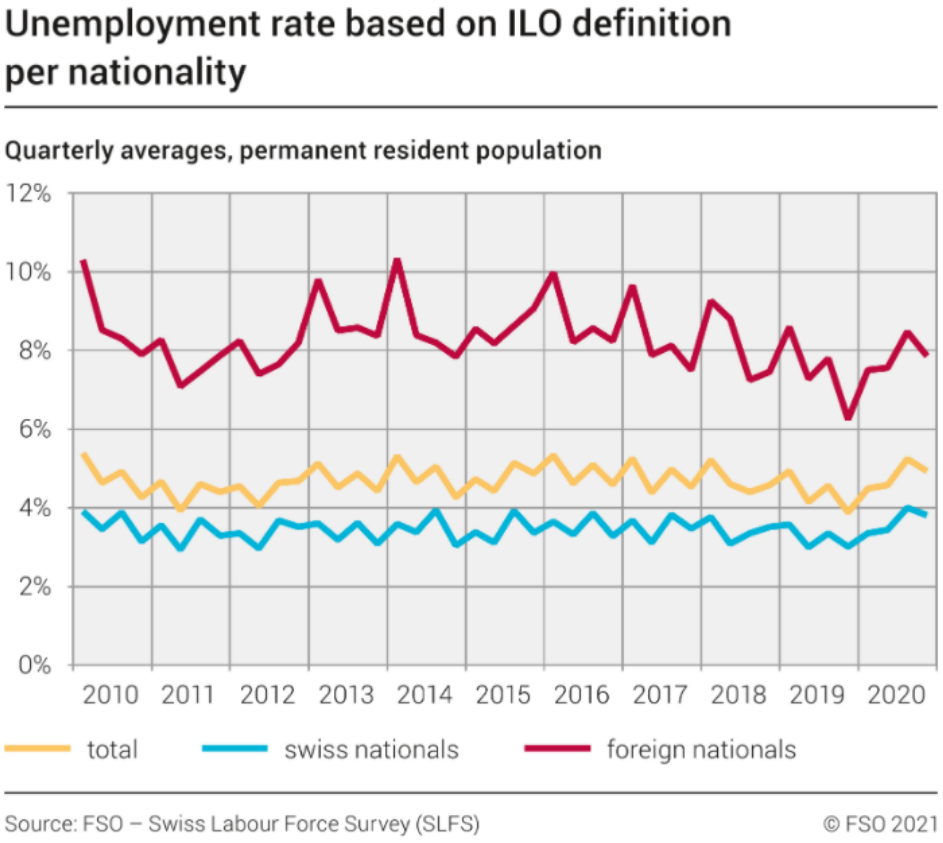


Figure 3-10: Unemployment Rate (FSO 2021a)

The job market is particularly important as it touches the essence of society as people and researchers are more concerned about job stability, the creation of new jobs, and the number of demolished jobs, as discussed previously.

Five different segments are identified and represented in five dependent variables to understand how technology advancement affects the future job market. The expectation is to get a comprehensive image of the near future job market in Switzerland and to know which segments will be more affected and in which direction.

These variables are total unemployment presented as a percentage of the total available labor force, unemployment amongst the male labor force, unemployment amongst female labor force, unemployment for people with only basic education (including secondary schools and profession-education), and finally, unemployment for people with advanced education (at least with a university degree). The forecast and analysis variables are presented in Table 3.7.

Table 3.7: List of Variables for Forecasting

Variable	**Indication**
Y1	Investments in information and communication technologies in millions of CHF
Y2	Gross Capital Formation in million CHF (current)
Y3	GDP Switzerland in million CHF (current)
Y4	Gross National Income (GNI) per capita in CHF
Y5	Healthcare Costs in millions of CHF
Y6	ICT goods imports (% total goods imports)
Y7	ICT service exports in millions of USD
Y8	Medium and high-tech exports (% manufactured exports)
Y9	New businesses registered (number)
Y10	Number of SMEs
Y11	Inflation, Date: Mai 2000 = 100
Y12	Labor Force Participation in the Labor market in full-time equivalents
Y13	Unemployment, total (% of the total labor force)
Y14	Unemployment, male (% of the male labor force)
Y15	Unemployment, female (% of the female labor force)
Y16	Unemployment with basic education (% of the total labor force with basic education)
Y17	Unemployment with advanced education (% of the total labor force with advanced education)
Y18	Employees in the retail sector
Y19	Male employees in the retail sector
Y20	Female employees in the retail sector
Y21	Workers in the healthcare sector
Y22	Nurses and midwives (per 1,000 people)
Y23	Employment in agriculture (% of total employment) (modeled ILO estimate)
Y24	Employment in industry (% of total employment) (modeled ILO estimate)
Y25	Employment in services (% of total employment) (modeled ILO estimate)

3.3.3 Forecast Methods

There are several possible techniques to conduct a forecast for economic and social purposes. One has to think of the aim of the forecast and who will be using the outcome of the forecast, and how it will be used. It is also necessary to determine the accuracy level required for the selected techniques (Chambers et al. 1971). Moreover, selecting a technique should accommodate what one has on hand and what one wants to achieve.

Some of the most common tools are Simple and Multi Linear Regression, Moving Averages, and Exponential Smoothing. Many relatively new platforms such as Amazon offer tools for forecasting like ARIMA and Prophet. Additionally, one should not outcount the Monte Carlo method when it comes to forecasting and especially for a simulation. Of course, there are other methods in statistics that serve the same purpose. All the mentioned methods have been considered and looked at carefully.

For this dissertation, several statistics and forecasting methods are selected. These are the Regression model, the Autoregressive (AR) model, Linear Multi-regression (LMR) model, Pearson Correlation Coefficient (PCC), Vector Autoregressive (VAR) Model, Exponential Smoothing ETS (error, trend, seasonal), and ARIMA models.

The available historic data is very small and limited to 20 reads. Most of the relevant data represent the years 2000 through 2020. Considering too old data will not serve the quality of the research because it is literary out of date. Society and ICT dependence is incomparable to the 1980s.

It is not always possible to tell which method is better than which; in some cases, different methods generate similar results. However, this is a clear time series analysis case, and the most suitable method is the ARIMA model, which has been dominant for many decades now (Veney and Luckey 1983). Nonetheless, other methods have been evaluated.

It is important to remember that this is a forecast that yields result with probabilities (for some methods), and there is always a margin for error. The method presentation will discuss more insight into the methods when necessary. Other insights will be discussed while showing results. The reason for the decentralization of information emission is the attempt to present the information once it is most needed and relevant, rather than having an information pool where the reader might be lost and unsure if the information is useful or needed.

The availability and data type play an important role in selecting a suitable forecasting method.

Understanding the correlation between the motivation variables ICT Investments and GCF Investments and the rest of the forecast variables is certainly interesting. Therefore, first, there will be a test using the Pearson correlation coefficient (PCC). Conducting the PCC test is relatively easily done using Microsoft Excel software. There is a need to clarify the meaning of correlation and causation. Once two variables are found to be correlated, they change in the same or opposite direction depending on whether the correlation is positive or negative. However, this does not necessarily imply that one variable is responsible for the changes in the other. For example, ice cream sales in summer rise significantly, and so does the number of sunburns in medical points. This example has a high correlation, but obviously, there is no causation. Eating ice cream will not cause sunburn.

One of the most common methods to forecast a variable independently is Exponential Smoothing and Linear regression. However, the Exponential Smoothing method is based on smoothing past data trends and might not be accurate enough for this forecast stage, especially since the second phase of the forecast will depend on this variable. Linear Regression fits even worse, as Linear regression decides the linear relation between timeline and values series, which makes it unsuitable for data with seasonality or cycles and not suitable for data that are not linear. In other words, Linear regression is too simplified for this forecast.

3.3.3.1 Considered Methods

More insight and explanation for the used methods, namely: Pearson Correlation Coefficient (PCC), Vector Autoregressive Model (VAR Model), R language, and Exponential Smoothing ETS, are provided in this section.

3.3.3.1.1 Pearson Correlation Coefficient (PCC)

Correlation defines the strength of a relationship between two variables and is completely symmetrical, meaning that the correlation between variable A and variable B is equal to the correlation between variable B and variable A. once there is a correlation between two variables, then this implies the if one variable changes to a certain extent, the other variable will also change.

The Pearson correlation is called the "product-moment correlation coefficient" (PMCC). It is referred to as "correlation" as well. It is often called Pearson Correlation Coefficient (PCC), also Pearson's r. This r symbol was originally "reversion", but it became later "regression" (Stanton 2001).

PCC is a statistical technique used when having two sets of data and calculating the linear correlation between them. Francis Galton developed the original idea in the late 19th century, then it was further improved by Karl Pearson and named after him (Stanton 2001). This method is likewise used for examining the relationship between two quantitative, continuous variables. The PCC formula produces a value between +1 and −1). The value +1 means a strong and total positive correlation between the two variables. The value -1 means a strong and total negative correlation between the two variables. The value 0 indicates no correlation between the two variables (or the two data sets). The equation for the Pearson correlation coefficient is below:

$$\mathrm{r} = \frac{\Sigma(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\Sigma(x_i - \bar{x})^2(y_i - \bar{y})^2)}}$$

r = correlation coefficient

x_i = values of the x-variable in a sample

$\bar{x}$ = mean of the values of the x-variable

y_i = values of the y-variable in a sample

$\bar{y}$ = mean of the values of the y-variable

Table 3.8 below shows the correlation between the two motive variables $y1$ and $y2$, and the rest of the forecast variables. It is important here to see the strength of the relationship in case there is a cause-and-effect relationship between the variables.

The green-colored cells indicate a high positive correlation. The darker the color, the stronger the correlation. On the other hand, the red-colored cells indicate a high negative correlation. The darker the color, the stronger the negative correlation.

Interpretation of PCC results

From the color scheme, employment in the retail sector has a high negative correlation with the two variables.

Table 3.8: Pearson Coefficient of Correlation

Forecast variables		**PCC**	
Variable description		with **ICT**	with **GCF**
#1	Investments in ICT in million CHF (current)	1.0000	0.9631
#2	Gross Capital Formation in million CHF (current)	0.9631	1.0000
#3	GDP Switzerland in CHF (current)	0.9492	0.9911
#4	Gross National Income (GNI) per capita in CHF (current)	0.9071	0.8992
#5	Healthcare Costs in millions of CHF	0.9303	0.9778
#6	ICT goods imports (% total goods imports)	-0.9174	-0.9241
#7	ICT service exports in millions of USD	0.9127	0.9397
#8	Medium and high-tech exports (% manufactured exports)	0.8976	0.8743
#9	New businesses registered (number)	0.8933	0.9244
#10	number of SMEs	0.8735	0.9522
#11	Inflation, Date: Mai 1993 = 100	0.9094	0.9024
#12	Labor Force Participation in the Labor market in full-time	0.5630	0.5528
#13	Unemployment, total (% of the total labor force)	0.5506	0.6682
#14	Unemployment, male (% of the male labor force)	0.4982	0.6114
#15	Unemployment, female (% of the female labor force)	0.5745	0.6902
#16	Unemployment with basic education (% of the total labor force with basic education)	0.6499	0.7748
#17	Unemployment with advanced education (% of the total labor force with advanced education)	0.6045	0.6966
#18	Employees in the retail sector	-0.8057	-0.8471
#19	Male employees in the retail sector	-0.6822	-0.7574
#20	Female employees in the retail sector	-0.7129	-0.7318
#21	Workers in healthcare and social services	0.9073	0.9679
#22	Nurses and midwives (per 1,000 people)	0.8350	0.8057
#23	Employment in agriculture (% of total employment)	-0.8366	-0.9073
#24	Employment in industry (% of total employment)	-0.9267	-0.8954
#25	Employment in services (% of total employment)	0.9336	0.9249

The assumption would be that they are strongly dependent on ICT advancement in society. In other words, more digitalization means jobs will be lost in this sector. On the other hand, ICT and high-tech goods exported and high-tech goods manufacturing will thrive with more digitalization and automation. The good news is that unemployment is not strongly correlated with $y1$, and $y2$. This means that the fears that jobs will disappear immediately are exaggerated. At least for Switzerland and in the short term. However, globally this is already observed as discussed before in chapter 3.1.7.

Income and GDP numbers are highly correlated with the two variables which is a positive thing for the economy. However, healthcare costs are expected to increase accordingly.

The last three variables are less relevant for the correlation test. The shift in the economy will continue as it was. The matter will be discussed in detail later.

The published research (Aldabbas et al. 2021) depended on the PCC test to segment variables for a forecast. The forecast focused on the quality of life in Switzerland for the near future. The variables with a correlation higher than 80% were forecasted together with ICT investment using a regression model. The rest of the variables were forecasted independently using Exponential Smoothing ETS. The findings say that the quality of life in Switzerland will generally not improve. For more details on the study, the reader is referred to (Aldabbas et al. 2021). The forecast in this dissertation is rather more sophisticated and the forecast method is more advanced.

3.3.3.1.2 Regression and R-squared Value

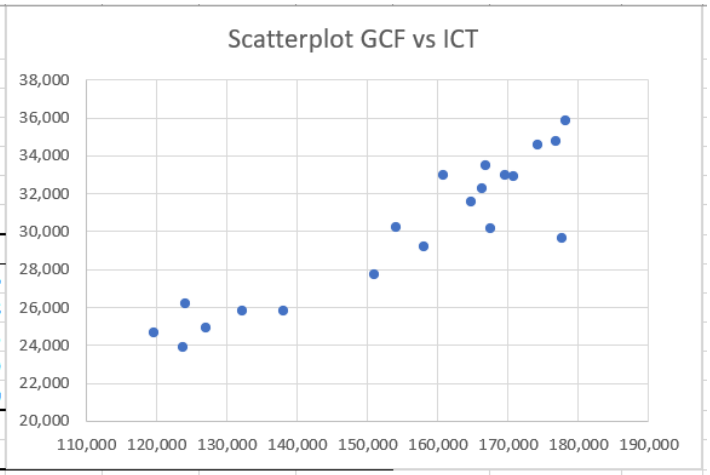
An equation can represent the relationship between two correlated variables (A and B) called the regression equation. Regression means that variable A is a function of variable B and changes when variable B changes. In other words, the regression tells how much a variable will change. One of the most important figures of regression statistics is the R-squared value which is the coefficient determination between the two variables. R-squared is a statistical measure to detect how close the data fit with the regression line.

R-squared gives a different insight into the relationship between the variables than the PCC. R-squared can be useful in this forecast to measure and estimate the suitability of the independent variable and its ability to explain the change in the dependent variables.

R-squared is always a value between 0 to 100%. The interpretation is like this: R-squared (as a percentage) of the variability of variable A is explained by the regression line / or by the regression of variable B on variable A. If R-squared = 0. This means that the regression model explains none of the variability of the variable (A or B). If R-squared =1, the regression model explains all the variability of the variable (A or B).

To better explain the R-squared value for this forecast, Figure 3-11 is an example of the regression model between "ICT investment" and "GCF investment".

Year	ICT Investment	GCF Investment
2000	24,917	127,086
2001	25,782	132,180
2002	26,164	124,089
2003	23,866	123,858
2004	24,658	119,651
2005	25,831	138,076
2006	27,725	150,988
2007	30,189	154,106
2008	31,547	164,708
2009	30,147	167,463
2010	29,214	158,111
2011	29,639	177,745
2012	32,260	166,381
2013	32,987	160,784
2014	32,877	170,834
2015	33,463	166,832
2016	32,995	169,676
2017	34,554	174,276
2018	34,745	176,909
2019	35,868	178,259
2020		187,515



SUMMARY OUTPUT								
Regression Statistics								
Multiple R	0.915296							
R Square	0.837768							
Adjusted R	0.828755							
Standard E	8339.319							
Observatic	20							
ANOVA								
	df	*SS*	*MS*	*F*	*ignificance F*			
Regressior	1	6.46E+09	6.46E+09	92.95195	1.56E-08			
Residual	18	1.25E+09	69544239					
Total	19	7.72E+09						
	Coefficients	*andard Erı*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*pper 95.0*
Intercept	8776.413	15291.16	0.573953	0.573102	-23349.1	40901.95	-23349.1213	40902
ICT Investr	4.882126	0.506384	9.641159	1.56E-08	3.818254	5.945999	3.818253608	5.946

Correlation	0.9153
R-squared	0.8378
p-value	0.000

Figure 3-11: Regression Model Example

The interpretation of R-squared: 83% of the variability of "GCF Investment" is explained by the regression line (or by regression of "ICT investment" of "GCF Investment"). This regression model indicates that the independent variable is suitable to be the measure for the dependent variable because R-squared is high. However, a high R-squared value does not necessarily mean that the model is accurate, and a low R-squared value does not indicate a problem. The desired value depends on the field of study.

3.3.3.1.3 Autoregression (AR Model) and Vector Autoregressive Model (VAR Model)

An autoregressive model is one in which the dependent variable is regressed on itself at least once. If an autoregressive model has one lag period, it follows a first-order autoregressive stochastic process, abbreviated AR (1). If the model comprises p delayed periods of the

dependent variable, it follows a (p)th-order autoregressive process, abbreviated AR (p) (Porter and Gujarati 2009). The forecast will depend massively on this model, as it is an element of the ARIMA models.

The VAR and AR models are part of time series models. Vector autoregression (VAR) is a statistical model and a forecasting algorithm applied to describe the relationship between several variables while they change for multivariate time series. The arrangement for the model is that every variable is a linear function of past lags of itself and past lags of the other variables (Pennsylvania State University 2021). This model is also an econometric tool for estimating several equations simultaneously (Lütkepohl 2005). To apply VAR models, there is no need for much prior knowledge about the factors that affect a variable. One must know what variables are hypothesized to affect other variables over time. For this dissertation, as noted before, the hypothesis is that the independent variable "Investments on ICT" is the influencing variable, and the rest of the variables are the affected variables. The following VAR model is used for the second phase of the forecast.

The Autoregression AR model equation for a variable Y is:

$$Y_t = \alpha + \beta_1 Y_{t-1} + \beta_2 Y_{t-2} + \cdots + \beta_p Y_{t-p} + \epsilon_t$$

r = correlation coefficient

Y_t = value of the dependent variable at time t

α = intercept (for this forecast $\alpha = 0$)

β_p = coefficients of the lags of Y till order p

ϵ_t = error (for simplicity $= 0$)

Hence, order p means: that the model uses up to p-lags of Y. These are the forecasters in the equation.

The vector autoregression VAR formula is between two interrelated variables as each affects the other.

$$Y_{1,t} = \alpha_1 + \beta_{11,1} Y_{1,t-1} + \beta_{12,1} Y_{2,t-1} + \epsilon_{1,t}$$
$$Y_{2,t} = \alpha_2 + \beta_{21,1} Y_{1,t-1} + \beta_{22,1} Y_{2,t-1} + \epsilon_{2,t}$$

Implementing the VAR model requires an advanced programming language such as R or Python. R, an open-source free programming language, is used for this forecast. R is a free software environment for statistical computing and graphics and a very strong tool for data analysis (Hornik 2020). R[3] was developed by Ross Ihaka and Robert Gentleman in 1993 and got its name from the first letter of their first names.

3.3.3.1.4 Multi-linear Regression MLR

The world is a complicated place. So, when looking for a variable prediction, it is generally more advantageous to employ more than one variable to generate that forecast. This results in multiple regression. Simple linear regression compares two models: one in which the independent variable does not exist, and the other uses the best-fit regression line. Adding more independent variables to a multiple regression procedure does not mean the regression is necessarily better or offers better predictions.

Adding more variables can explain more variation but creates other problems. It can sometimes make things worse, which is called overfitting. The idea is to pick a suitable model.

Adding more independent variables creates more relationships among them. Consequently, not only the independent variables will be potentially related to the dependent variables, but they can also be related to each other. When this happens, it is called multicollinearity.

Ideally, the independent variables are correlated with the dependent variables but not with each other. The problem with multicollinearity is that one cannot be sure which independent variables explain the variation in the dependent variables.

In multiple regression, there is no error in the model formula. The coefficient is interpreted as the estimated change in y corresponding to a one-unit change in a variable when all other variables are held constant.

If the independent variables are highly correlated, they should not be used in the multiple regression as they are redundant. The correlation is significant if $p < 0.05$. If $R > 0.95$, then the variables are multicollinear and cannot be included in the regression.

[3] For further information on R, the website is accessible at www.r-project.org

Figure 3-11 from the example before shows the scatterplot for the independent variables. A high correlation is noticed after the regression analysis, and the p-value is $p = 0.000 < 0.05$ which means that the correlation is significant and there might be a multicollinearity problem. However, $R = 0.90 < 0.95$ so it is possible to use both independent variables for the regression model.

To consider any regression to be real and that the independent variable is strongly related to the dependent variable, all the relevant p-values must be below the threshold of 0.05. That implies that later, in the multi-linear regression model, one has to look carefully at all p-values. First, the model's p-value must be below 0.05 to consider the model significant. Then one can look at the p-values of each independent variable to validate their regression in the model. If a p-value for any of the variables is higher than 0.05, then the variable must be ignored and considered irrelevant to the regression model. A new regression will have to be made for the dependent variable and the remaining independent variable.

Hence, often, one of the following three threshold values can be considered significant for the p-value. These values are 0.05, 0.01, 0.001. their interpretation is in Table 3.9 (Schmidt and Osebold 2017). The lower the threshold is, the stricter the model is.

Table 3.9: Significance Levels for p-value

Significance level	Specification
$\boldsymbol{p > 0.05}$	Not significant
$\boldsymbol{p <= 0.05}$	Significant
$\boldsymbol{p <= 0.01}$	Very significant
$\boldsymbol{p <= 0.001}$	Highly significant

Throughout this dissertation, the used threshold value for p is 0.05 which is also the most used in literature.

One last remark on the p-values for the linear regression model: If the p-value for the intercept is less than 0.05, then the intercept is significantly different from zero. Otherwise, If the p-value is greater than the significance level of 0.05, the intercept is not significantly different from zero (Frost 2019).

3.3.3.2 Selected Methods

In addition to the Exponential Smoothing ETS, regression and ARIMA models are generally suitable for this kind of forecast, and the results they generate are close enough depending on the type of application and the setup configuration (Veney and Luckey 1983). In a recently published paper (Aldabbas et al. 2021), forecasting quality of life, the forecast used a regression model. The results are similar to the ones obtained using the ARIMA model. Hence, to serve this dissertation's purpose, the exact numbers of the forecast are not what most matter. It is rather the direction of the evolution of the figures for society.

For this dissertation, the focus will be only on using Exponential Smoothing ETS and applying ARIMA models.

3.3.3.2.1 Exponential Smoothing ETS

In time series analysis, there are several models. The first model used in this dissertation is the Exponential Smoothing Model. It is referred to as ETS Model, which means Error, Trend, and Seasonality. The Exponential Smoothing forecast uses weighted averages of past observations giving more weight to the last observation. The weight gets smaller as the observation gets older. This model is popular because of its calculation simplicity and the availability of its application using software like MS Excel. Determining how to apply the error, trend, and seasonality terms starts with visualizing the data by using time series decomposition plot. This plot separates the time series into its seasonal, trend, and error (residuals) components, as seen in Figure 3-12 (Brownlee 2017).

The Exponential Smoothing (ETS) method is a statistical algorithm for time-series forecasting (Amazon Forecast 2021). This method is based on smoothing historic data trends and other prior assumptions, and it provides somehow accurate forecasts on the test set. This algorithm detects seasonality patterns and confidence intervals to perform smoothing. The Exponential Smoothing method is a member of the ETS model's family. "E" stands for error, "T" stands for trend, and "S" stands for seasonal. The model can be defined as Exponential smoothing (Tran et al. 2020).

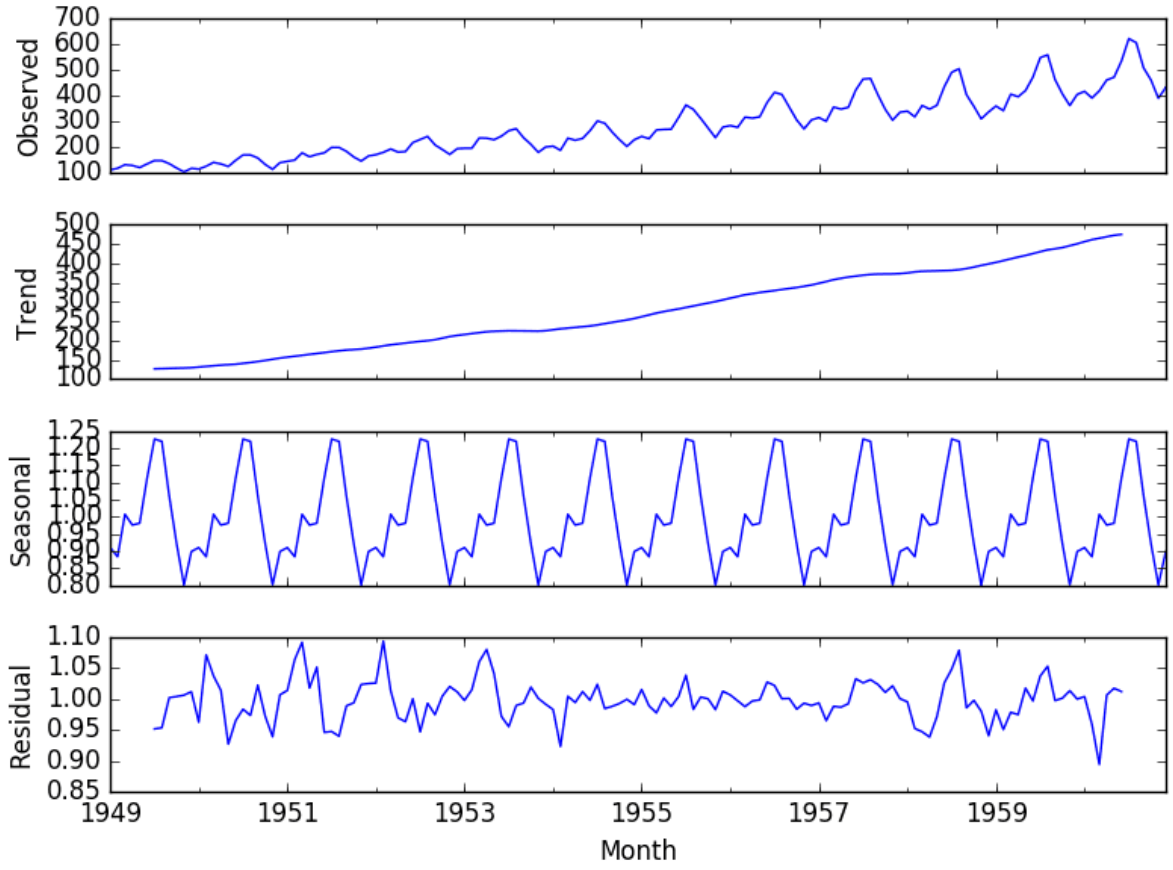


Figure 3-12: Example of Time Series Decomposition Plot (Brownlee 2017)

The equation for simple exponential smoothing is in the equation. More simply: s_t is a simple weighted average of the current read x_t and the previous smoothed forecast s_{t-1}

$$s_t = \alpha x_t + (1 - \alpha) s_{t-1}$$

s_t is the current forecast read

α is the smoothing factor and $0 \leq \alpha \leq 1$

x_t is the actual data read

s_{t-1} forecast from the previous period

It is easily observable that this forecasting method puts much weight on the previous read, which is another reason to implement the VAR Model for the forecast.

The Exponential Smoothing ETS is easily run on Microsoft Excel by selecting the data and the function forecast. Unlike VAR Model, Exponential Smoothing ETS does not require advanced programming software for implementation like R or Python.

The outcomes of this method on MS Excel are three charts, the upper confidence bound, the lower confidence bound, and the forecast itself. The confidence interval for the entire forecast is 95%. It means that 95% of future values are expected to fall within this radius from the forecasted result. For the variables that showed a high correlation with the independent variable, the upper and lower bounds are not necessary to be presented in the forecast. However, for the variables that show a low correlation with the independent variable, the upper and lower bounds will be presented for more clarity and insight into the forecast.

3.3.3.2.2 ARIMA Models

Time series forecasting predicts future values of a particular quantity based on previously observed values. In other words, it uses statistical models to predict future values based on past observations. Examples are annual population growth, stock market prices, future delivery demand, or sales figures. The measured data should have sequential and equal intervals. Once the data is collected, there are two objects to investigate. First: Identify the patterns represented by the sequence of observations. Second, predicting future values of the time series.

In time series analysis, data consists of a systematic pattern, usually a set of identifiable components and random noise, which is the error. Random noise usually makes the patterns difficult to identify. Therefore, most techniques in time series analysis involve some form of filtering the noise to make the pattern more notable.

There are two types of time series: stationary and non-stationary. If the mean and the variance of all the data points are constant over time, then the series is stationary. Otherwise, the series is non-stationary, and a certain procedure has to be done to convert the non-stationary series into stationary series. This procedure is called differentiation. Without differentiation, it is not possible to go on with the forecasting for non-stationary series.

The characteristics of a stationary series imply that the series' means should not be a function of time but rather a constant. The variance of the series should not be a function of time. Finally, the covariance of the (i)th term and the (i+m)th term should not be a function of time.

Time series data varies with time, and many factors play into this variation. These factors are components of the time series data. They are trends, seasonal variations, cyclic variations, and irregular variations.

Forecasting future values of a time series requires the following steps to come into play: investigating and cleaning the dataset, determining trends and seasonal components, applying the findings to a suitable model, and finally, forecasting the needed values.

The collected data should be plotted in a graphical presentation that shows the relationship between the time and time series target variable. The time should be on the horizontal access, and the variable in the study is on the vertical access. Visual analysis and looking at the graphs are very important for time series analysis. This is where trends can be detected. A trend is a gradual shift of movements into a relatively higher or lower value over a long period of time. There are upward trends and downward trends. If there is no trend of such nature, then it is called a stationary trend. If the time series experience upward and downward trends, this case is called cyclical. Seasonality can be spotted at this visual stage as well. Seasonality is a regularly occurring trend that keeps happening over time.

Cyclical patterns differ from seasonality. Cyclical patterns do not have a fixed period, while seasonality is unchanging and associated with some aspect of the year calendar. Cyclical patterns have a longer cycle length, while seasonality has a shorter cycle length. The magnitude of the cycle changes more for the cyclical pattern than for the seasonality. A typical example of a cyclical pattern is the stock market. Bookings in ski resorts have a clear seasonality character.

The ARIMA model is a type of statistical model used for evaluating and forecasting time series data. It stands for Autoregressive Integrated Moving Average. The model is used when the data shows evidence of non-stationarity. A random variable is considered stationary if the statistical properties are constant over time. A stationary series has no trend; the variations around the mean have a constant amplitude and change consistently. That implies that the autocorrelations remain constant over time. A time series can be seen as a combination of signal and noise. So, the ARIMA model is considered a filter that separates the signal from the noise. The signal will then be generalized to forecast future values.

ARIMA forecasting equation is a linear equation where the predictors consist of lags of the dependent variable and/or lags of the forecast errors. In other words, a predicted value is composed of a constant, a weighted sum of one or more recent observed values, and a weighted sum of one or more recent error values.

By breaking down the parts of the acronym ARIMA:

- AR (Autoregressive) uses the dependent relationship between an observation and a number of lagged observations.
- I (Integrated) the use of raw observation differencing. This is used to stabilize the time series.
- MA (Moving Average) - applies the dependence between observation and residual errors from a moving average model to lag observation.

Each of these components is specified in the model as a parameter. $AR\ (P)\ =$ Lag order. $I(d)\ =$ differencing degree. $MA(q)\ =$ moving average order.

Steps to build the ARIMA model:

AKA Box-Jenkins Method (Box et al. 2016) is a stochastic model-building process that consists of three steps:

- Identification: using the data to select the subclass of the model

- Estimation: utilize the data to train the model's parameters.

- Diagnostic checking: assessing the fitted model considering the given data.

Further details on Identification:

It is done by running the Unit Root Test to assess whether the time series is stationary and, if not, how many differences are required to make it stationary. Then comes identifying the parameters of an ARIMA model for the data by analyzing the Autocorrelation Function (ACF) and the Partial Autocorrelation Function (PACF).

The Autocorrelation Function (ACF) plot depicts an observation's correlation with lag values, where the x-axis represents the lag and the y-axis represents the correlation values, whether positive or negative.

The Partial Autocorrelation Function (PACF) graphic summarizes the correlations for observation with lag values that are not accounted for by the previously lagged observation.

If the ACF fades off after a lag and the PACF has a firm cut-off after a lag, the model is AR. The value for p is assumed to be this latency.

If the PACF lags after a lag and the ACF has a sharp cut-off after the lag, the model is MA. The q values make up this lag.

If both ACF and PACF decline, the model is a combination of AR and MA.

The estimating process entails employing numerical methods to reduce a loss or error term.

Looking for evidence that the model is not a good match for the data is part of the diagnostic process. Overfitting and residual errors are two topics to look at. Overfitting occurs when the model becomes more sophisticated than necessary and catches random noise in the training data. This has a detrimental influence on the model's capacity to generalize, resulting in poor forecast performance on out-of-sample data. Both in-sample and out-of-sample performance must be carefully monitored.

Forecast residuals give a great opportunity for diagnostics in situations of residual errors. A review of error distributions aids in the removal of model bias. An ideal model's mistakes would mimic white noise, which is a Gaussian distribution with a mean of zero and symmetrical variance. For that, one can use histograms or density plots that compare the distribution of errors to the expected distribution. In the case of a non-Gaussian distribution, the data might need pre-processing. A skew in the distribution or a non-zero mean suggests a potential bias in the forecast that must be rectified.

The time series of forecast residuals produced by the case of an ideal ARIMA model has no temporal structure. ACF and PACF graphs of the residual error time series are necessary to verify this. The presence of serial correlation in the residual errors indicates that this input should be used in the model.

ARIMA stands for Autoregressive integrated moving average. Popularly known as Box-Jenkins's (1976) methodology. It is one of the most applied methods in forecasting variables which obtains its inputs from the variable itself to forecast its future values. The variable is regressed on its historic values.

ARIMA contributes to helping investors, policymakers, governmental plans, stakeholders, and many other categories of people make informed decisions.

Underlying assumptions for ARIMA models

- Stationarity (for AR models): A series is considered stationary when it exhibits mean reversions, has a finite and time-invariant variance, and has a correlogram that diminishes as the lag length increases.
- Invertibility (for MA models): It is necessary that the series can be represented by a finite order MA or convergent autoregressive process. The autocorrelation function (ACF) and the partial autocorrelation function (PACF) must be usable for identification. Finally, the series should be approximated by an autoregressive model.

Model specification

The Box-Jenkins time series models allow Y_t to be explained by past, or lagged values of Y itself and stochastic error terms (referred to as shocks). The series is simply explaining itself through its historic data. ARIMA models are composed of two distinct models that attempt to describe the behavior of the series from two different perspectives: Autoregressive models (AR) and Moving Average models (MA)

$$gdp_t = a + b * gdp_{t-1} + u_t$$

The equation states that gdp in time t is explained by the immediate past value in time $(t-1)$ and a white noise error term u. The future value of gdp is time $(t+1)$ is largely dependent on the behavior of the series in the present time t.

The generalized $AR(p)$ model:

The autoregressive model can be generalized to include several lags of the series, as in the examples below

$$AR(2): gdp_t = a + b_1 gdp_{t-1} + b_2 gdp_{t-2} + u_t$$

$$AR(3): gdp_t = a + b_1 gdp_{t-1} + b_2 gdp_{t-2} + b_3 gdp_{t-3} + u_t$$

$$AR(p): gdp_t = a + \sum_{i=1}^{p} b_i gdp_{t-i} + \mathrm{u_t}$$

In the $MA(1)$ model, just as in $AR(1)$ model, the simplest of the moving average models is the first-order moving average, $MA(1)$, which takes the form:

$$gdp_1 = y + d_0 u_t + d_1 u_{t-1}$$

Where gdp is explained by the value of the error term and the immediate past error known at time t.

The generalized $MA(q)$ model:

The moving average (MA) model can be generalized to include more lags of the error term like in the examples below

$$MA(2): gdp_t = y + d_0 u_t + d_1 u_{t-1} + d_2 u_{t-2}$$

$$MA(q): gdp_t = y + d_0 u_t + \sum_{j=1}^{q} d_j u_{t-j}$$

From both $AR(p)$ and $MA(q)$ models, the $ARMA(p, q)$ model for the gdp can be written as follows

$$ARMA(p, q): gdp_t = a + \sum_{i=1}^{p} b_i gdp_{t-i} + d_0 u_t + \sum_{j=1}^{q} d_j u_{t-j}$$

The model contains p lags of the dependent variable and q lags of the error term.

The distinction between $ARMA$ and $ARIMA$ models is the integration component which is related to stationarity. In practice, most economic variables are non-stationary and have to go through transformation via differencing to become stationary. The transformation process is also called integration. So, by looking at any $ARIMA$ model, the reader can notice whether or not the series has gone through the integration process before the analysis.

$ARIMA(p, d, q)$ indicates that the model has (p) lags of the dependent variable, and it is gone through (d) times of differencing to become stationary, and it has (q) lags of the error term.

3.3.4 Application of ARIMA Model and Exponential Smoothing ETS

The first application of the forecasting methods will be made with some details on the GDP using both Exponential Smoothing ETS and ARIMA models. The rest of the forecast variables will be without repeated explanation.

3.3.4.1 ARIMA Modeling

Modeling GDP in Switzerland using the ARIMA model. GDP's historic data is presented as SER01 in millions of CHF in Figure 3-13.

Introduction ARIMA (p,d,q) model, explaining the Box-Jenkins procedures, will be added.

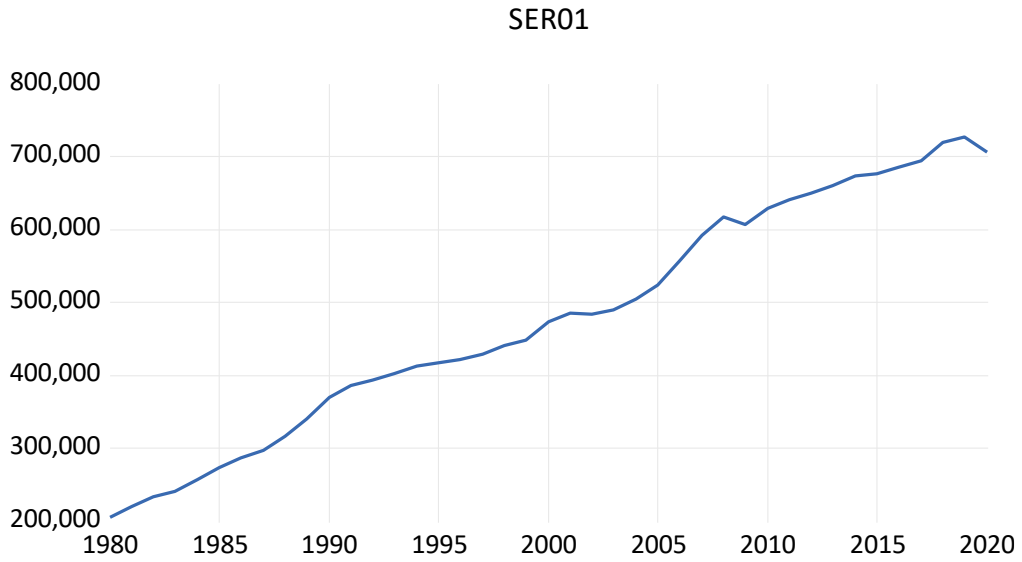


Figure 3-13: GDP Historic Data

The available historic data is from the year 1980 through the year 2020 in a million Swiss francs (in current price). The detailed data are presented in Table 3.10. Hence, the GDP figure for 2021 was not yet published by the time of doing this analysis.

Table 3.10: GDP Complete Data

Year	GDP	Year	GDP	Year	GDP	Year	GDP
1980	205,543	**1991**	385,929	**2002**	483,440	**2013**	660,649
1981	220,657	**1992**	393,957	**2003**	488,937	**2014**	672,818
1982	233,769	**1993**	402,596	**2004**	504,278	**2015**	675,736
1983	240,831	**1994**	412,537	**2005**	523,663	**2016**	685,441
1984	257,403	**1995**	417,579	**2006**	556,439	**2017**	693,694
1985	272,919	**1996**	420,822	**2007**	592,442	**2018**	719,272
1986	286,428	**1997**	428,310	**2008**	617,696	**2019**	727,212
1987	297,351	**1998**	440,569	**2009**	607,377	**2020**	706,242
1988	315,666	**1999**	448,437	**2010**	629,325	**2021**	
1989	340,727	**2000**	472,596	**2011**	641,200		
1990	369,509	**2001**	484,723	**2012**	648,981		

The first task is to determine the stationarity of the time series SER01 as shown in Figure 3-13. For that, the Dicky-Fuller test is run.

Unit root (Deterministic Trend)

From Figure 3-13, this series has an increasing trend over the years and is certainly not stationary as a linear trend is appearing (this will be proven with calculations first. Now, it is only a visual illustration). By looking at the first-order differencing in Figure 3-14, the plot has a constant mean of 12'000 (millions) and a big variance of 109,690,414. Even looking at the first differencing using a natural logarithm does not appear to make a lot in terms of changing the first difference variable. This is shown in Figure 3-15.

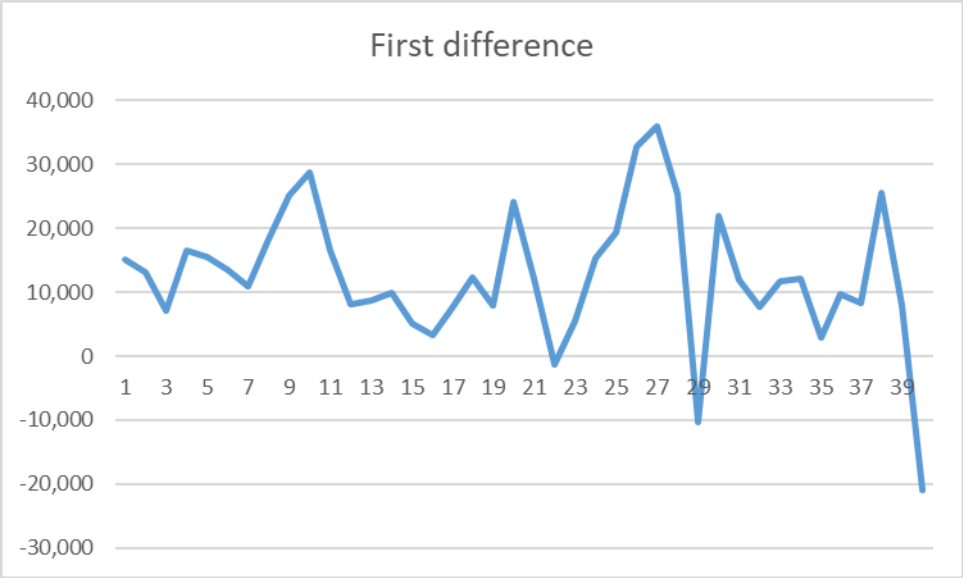


Figure 3-14: First Order Difference SER01

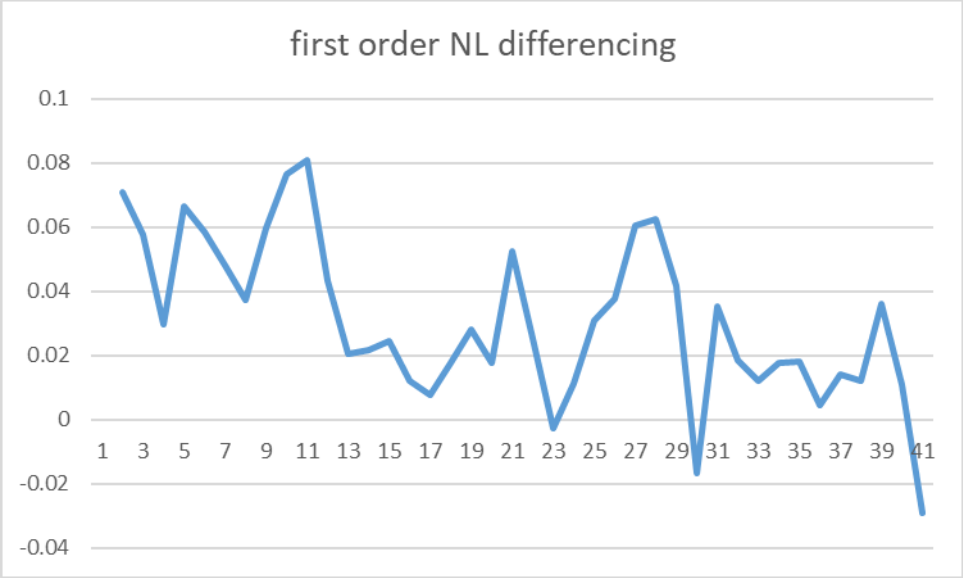


Figure 3-15: First Order Difference Natural Logarithm Transformation SER01

Nevertheless, the series is stationary after taking the first-order differencing.

Now to the test part: The following outcomes in Figure 3-16 are the results of the Dicky-Fuller test.

The p-value (0.623) is higher than 0.05. This means that the series is nonstationary as we cannot reject the null hypothesis H0 SER01 has a unit root.

Also, the absolute value of the t-test is smaller than the t-value at 0.05. which indicates the same outcome: SER01 is nonstationary.

Null Hypothesis: SER01 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=9)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-1.292181	0.6239
Test critical values:	1% level	-3.605593	
	5% level	-2.936942	
	10% level	-2.606857	

*MacKinnon (1996) one-sided p-values.

Augmented Dickey-Fuller Test Equation
Dependent Variable: D(SER01)
Method: Least Squares
Date: 12/13/21 Time: 16:21
Sample (adjusted): 1981 2020
Included observations: 40 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
SER01(-1)	-0.013822	0.010696	-1.292181	0.2041
C	19040.42	5314.820	3.582514	0.0010

R-squared	0.042091	Mean dependent var	12517.48
Adjusted R-squared	0.016883	S.D. dependent var	10606.37
S.E. of regression	10516.46	Akaike info criterion	21.40798
Sum squared resid	4.20E+09	Schwarz criterion	21.49242
Log likelihood	-426.1596	Hannan-Quinn criter.	21.43851
F-statistic	1.669731	Durbin-Watson stat	1.325787
Prob(F-statistic)	0.204098		

Figure 3-16: Dicky-Fuller Test SER01

By doing the Dickey-Fuller test, taking the 1st difference in Figure 3-17, we notice that the p-value of 0.007 is smaller than 0.05

We reject the null hypothesis, and we say that the series is stationary at the first difference: $I(1)$.

Null Hypothesis: D(SER01) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=9)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-3.744182	0.0071
Test critical values:	1% level	-3.610453	
	5% level	-2.938987	
	10% level	-2.607932	

*MacKinnon (1996) one-sided p-values.

Augmented Dickey-Fuller Test Equation
Dependent Variable: D(SER01,2)
Method: Least Squares
Date: 12/13/21 Time: 16:34
Sample (adjusted): 1982 2020
Included observations: 39 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
D(SER01(-1))	-0.690165	0.184330	-3.744182	0.0006
C	8306.501	2983.211	2.784416	0.0084

R-squared	0.274779	Mean dependent var	-925.2308
Adjusted R-squared	0.255178	S.D. dependent var	12152.08
S.E. of regression	10487.62	Akaike info criterion	21.40370
Sum squared resid	4.07E+09	Schwarz criterion	21.48901
Log likelihood	-415.3721	Hannan-Quinn criter.	21.43431
F-statistic	14.01890	Durbin-Watson stat	1.641766
Prob(F-statistic)	0.000614		

Figure 3-17: Dicky-Fuller Test (1st Differencing) SER01

The next step is to analyze the correlogram to detect the ARIMA model's p (autoregression) and q (moving average) parameters. Because of the apparent non-seasonality, only ARIMA(p, d, q) model is considered.

The outputs of ACF and PACF correlograms are shown in Figure 3-18 and Figure 3-19 respectively. But the outputs show insignificance! Hence, 1st order differencing must be taken.

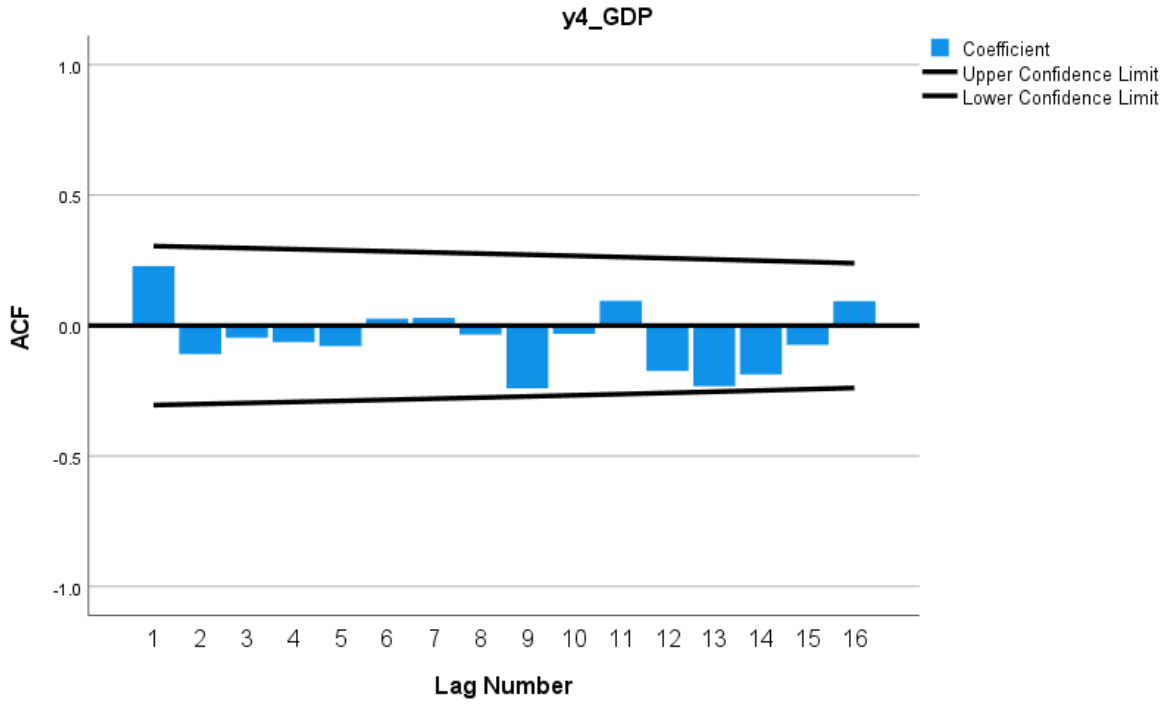


Figure 3-18: ACF Correlogram SER01

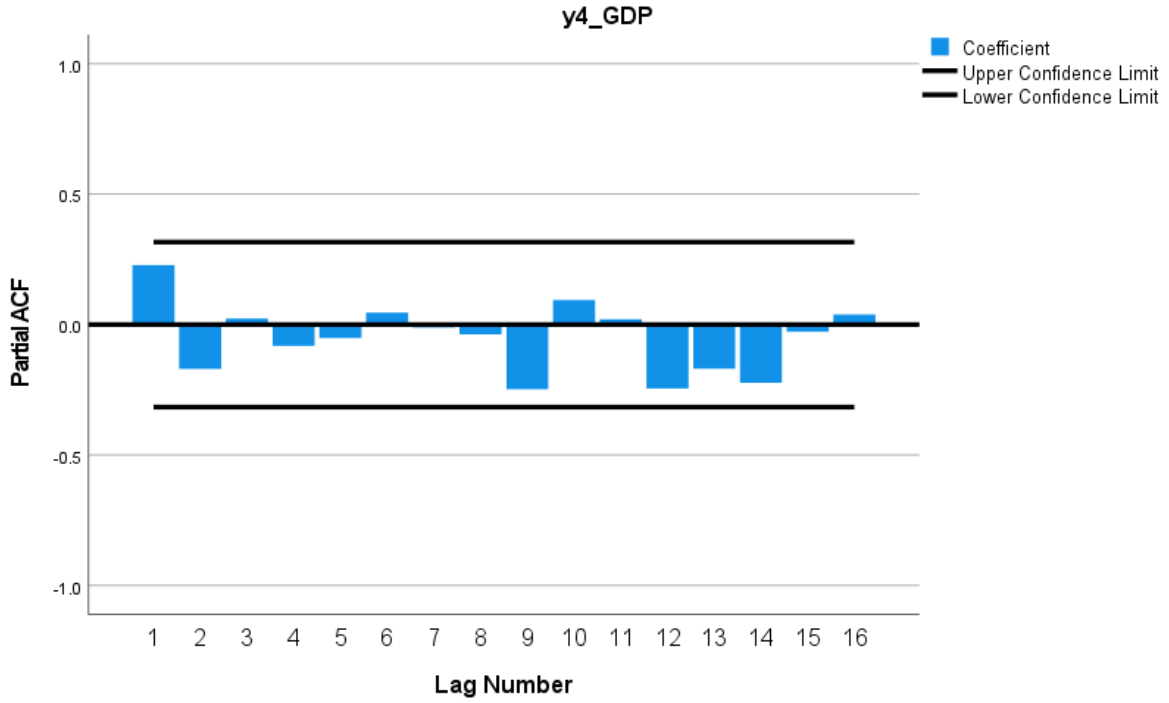


Figure 3-19: PACF Correlogram SER01

Due to the insignificance of the correlogram output, the natural logarithm transformation will be considered when producing the new correlogram.

The correlograms accordingly (1st level difference $I = 1$ and NL transformation) are in Figure 3-20 and Figure 3-21.

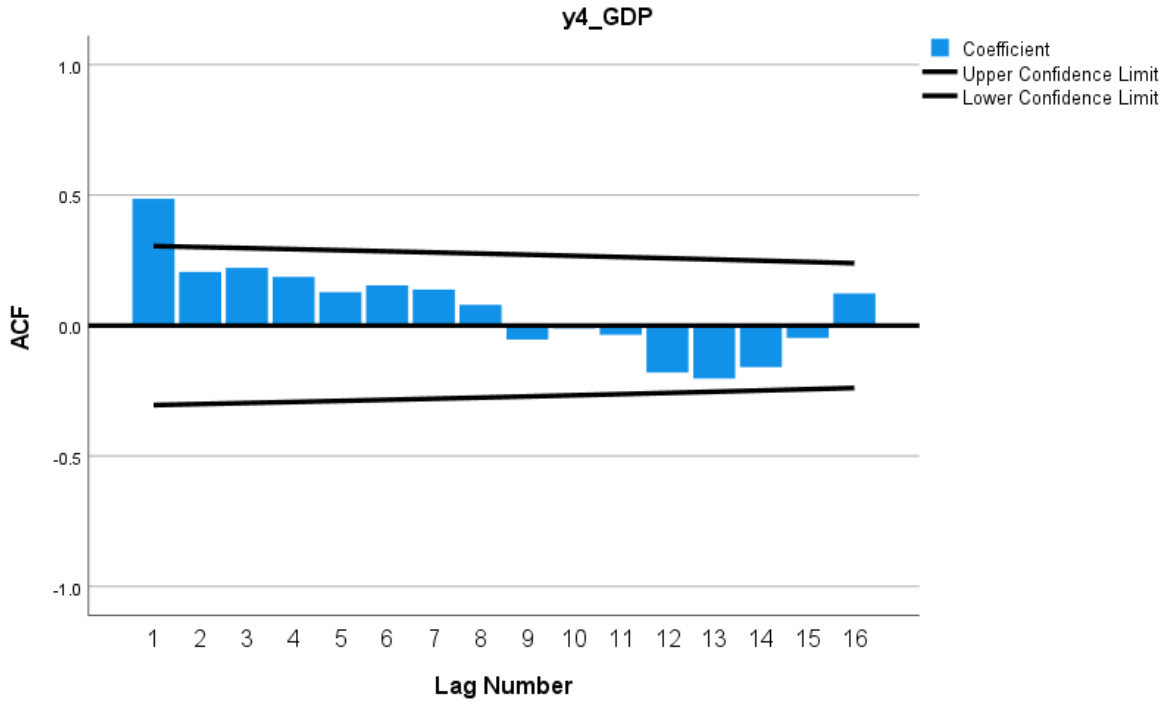


Figure 3-20: ACF Correlogram NL Transformation

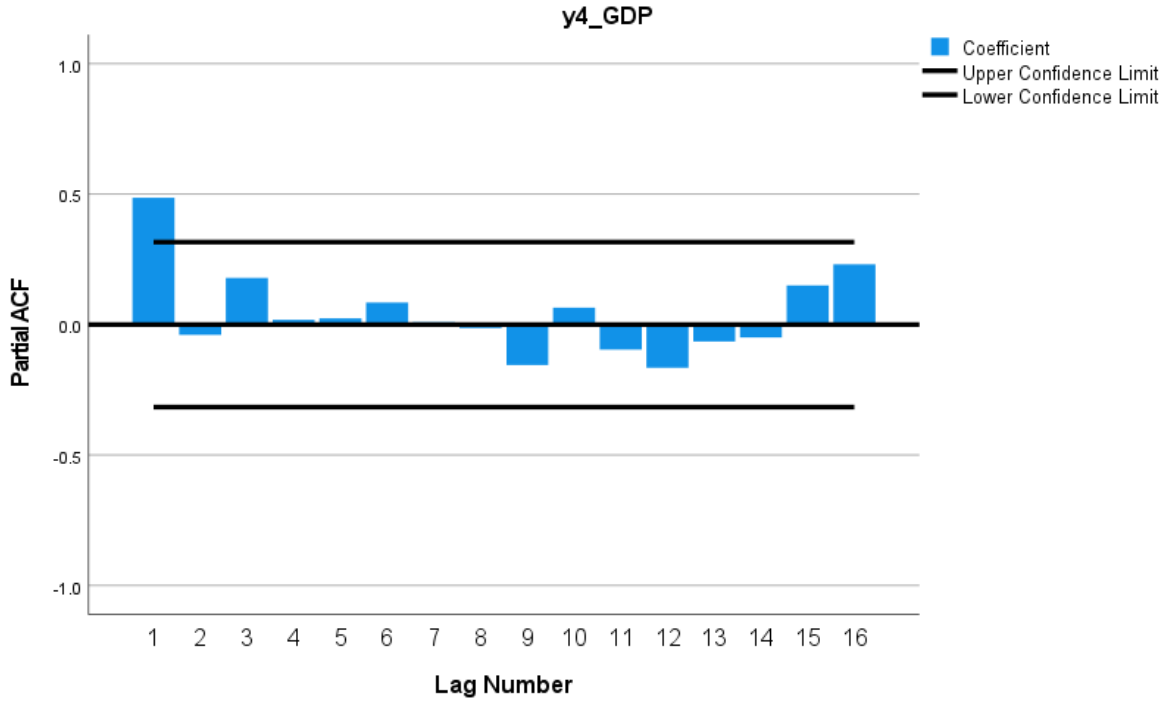


Figure 3-21: PACF Correlogram NL Transformation

Analyzing the correlogram which produces the tables of the AC (autocorrelation) and PAC (partial autocorrelation) as from Figure 3-20 and Figure 3-21:

- Autocorrelation: only the first autocorrelation coefficient is different from zero. The ACF has a cutoff after lag 1. Therefore, the autocorrelation of order 1 is identified. $p = 1$
- Partial correlation: only the first correlation coefficient is different from zero. The PACF has a cutoff after the first lag. Therefore, a moving average process of order $q = 1$ is identified

Both p and q parameters for the ARIMA model can be 1.

However, the following variation of ARIMA models should be considered.

ARIMA (1,1,1)

ARIMA (0,1,1)

ARIMA (1,1,0)

The values of the first model (1,1,1) in Figure 3-22 show insignificant p values for the coefficients of AR and MA. Therefore, the model is not good.

Dependent Variable: D(LGDP)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 12/15/21 Time: 10:30
Sample: 1981 2020
Included observations: 40
Convergence achieved after 17 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.013134	0.003294	3.987284	0.0003
AR(1)	0.461190	0.350427	1.316080	0.1965
MA(1)	0.193299	0.327284	0.590617	0.5585
SIGMASQ	7.98E-05	1.86E-05	4.283417	0.0001

R-squared	0.305167	Mean dependent var	0.013401
Adjusted R-squared	0.247264	S.D. dependent var	0.010853
S.E. of regression	0.009416	Akaike info criterion	-6.386915
Sum squared resid	0.003192	Schwarz criterion	-6.218027
Log likelihood	131.7383	Hannan-Quinn criter.	-6.325850
F-statistic	5.270327	Durbin-Watson stat	1.866071
Prob(F-statistic)	0.004066		

Inverted AR Roots	.46
Inverted MA Roots	-.19

Figure 3-22: ARIMA (1,1,1) GDP

The second model (0,1,1) in Figure 3-23 is potentially suitable.

Dependent Variable: D(LGDP)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 12/15/21 Time: 10:32
Sample: 1981 2020
Included observations: 40
Convergence achieved after 17 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.013269	0.002158	6.149117	0.0000
MA(1)	0.519505	0.131468	3.951573	0.0003
SIGMASQ	8.45E-05	2.12E-05	3.992276	0.0003

R-squared	0.264138	Mean dependent var	0.013401
Adjusted R-squared	0.224361	S.D. dependent var	0.010853
S.E. of regression	0.009558	Akaike info criterion	-6.382880
Sum squared resid	0.003380	Schwarz criterion	-6.256214
Log likelihood	130.6576	Hannan-Quinn criter.	-6.337081
F-statistic	6.640569	Durbin-Watson stat	1.605236
Prob(F-statistic)	0.003434		

Inverted MA Roots	-.52

Figure 3-23: ARIMA (0,1,1) GDP

The third model (1,1,0) in Figure 3-24 is slightly better than the second model because the R-squared value is higher.

Dependent Variable: D(LGDP)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 12/15/21 Time: 10:31
Sample: 1981 2020
Included observations: 40
Convergence achieved after 7 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.013101	0.003297	3.973276	0.0003
AR(1)	0.597796	0.151606	3.943089	0.0003
SIGMASQ	8.04E-05	1.78E-05	4.514874	0.0001

R-squared	0.300091	Mean dependent var	0.013401
Adjusted R-squared	0.262258	S.D. dependent var	0.010853
S.E. of regression	0.009322	Akaike info criterion	-6.429782
Sum squared resid	0.003215	Schwarz criterion	-6.303116
Log likelihood	131.5956	Hannan-Quinn criter.	-6.383983
F-statistic	7.931997	Durbin-Watson stat	1.779197
Prob(F-statistic)	0.001359		

Inverted AR Roots	.60

Figure 3-24: ARIMA (1,1,0) GDP

The final selected model of the LGDP sequence is ARIMA (1, 1, 0).

Residuals correlograms in Figure 3-25 and Figure 3-26 show no values with statistical significance. This is called white noise. This means that the model is good.

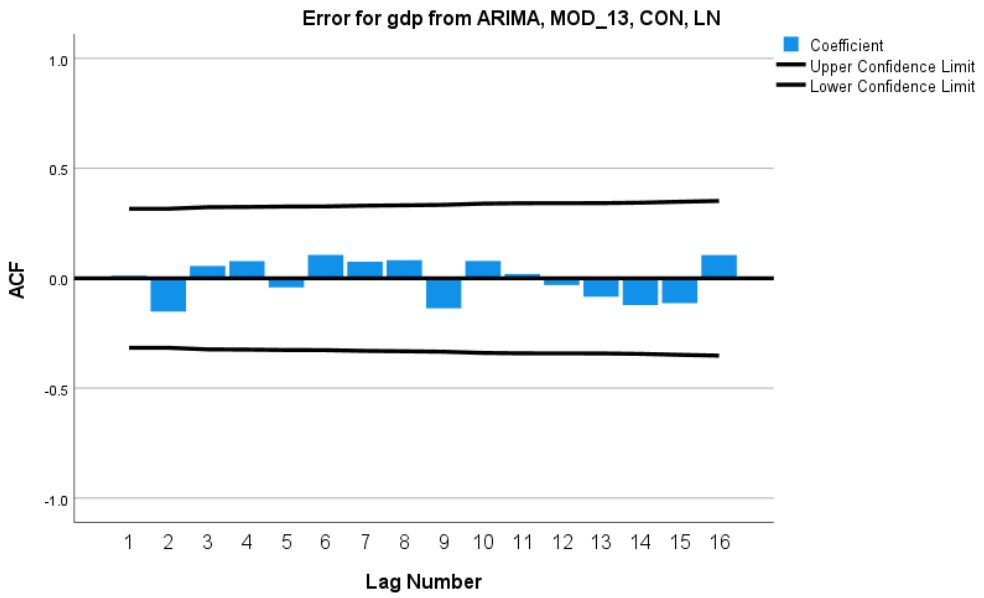


Figure 3-25: Residuals Correlogram ACF

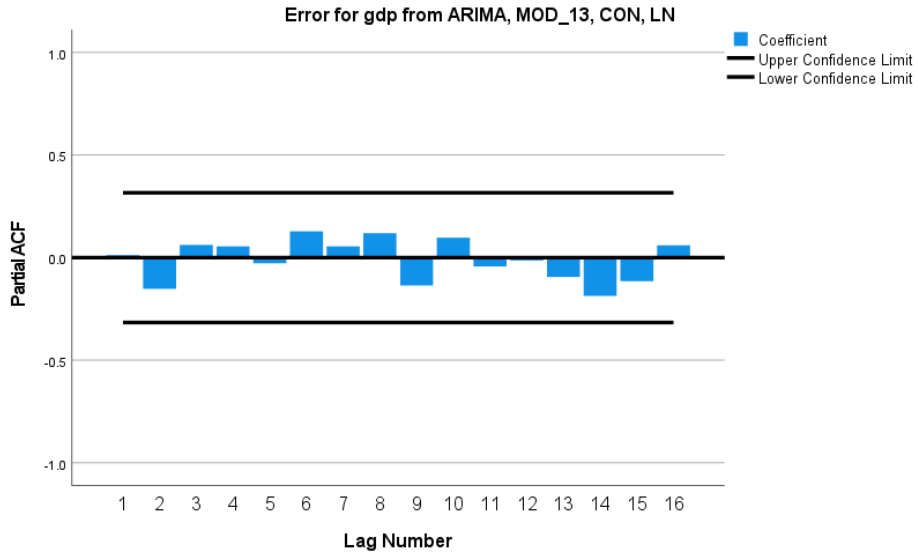


Figure 3-26: Residuals Correlogram PACF

The ARIMA (1,1,0) is a suitable model for forecasting the GDP of Switzerland.

It is found that $\mu = 0.013101$ $\theta_1 = 0.597796$ $a_t = 0$

The first difference of the logged GDP is stationary AR (1) model

$y_t = \log(z_t)$

$\Delta y_t = x_t$

$x_t = \mu + \theta_1 x_{t-1} + a_t$

$$x_t = 0.013101 + 0.597796\, x_{t-1}$$

The forecasted values for the next decade as per the model ARIMA (1,1,0) are in Table 3.11 and the fitted model is in Figure 3-27.

Table 3.11: Forecasted GDP Values

Year	Forecast	Lower Bounds	Upper Bounds
2021	702627	672985	733244
2022	709336	653742	768432
2023	722457	641983	810333
2024	739733	635599	856276
2025	759834	633086	904887
2026	781969	633410	955469
2027	805665	635867	1007689
2028	830646	639975	1061420
2029	856750	645402	1116645
2030	883889	651918	1173412

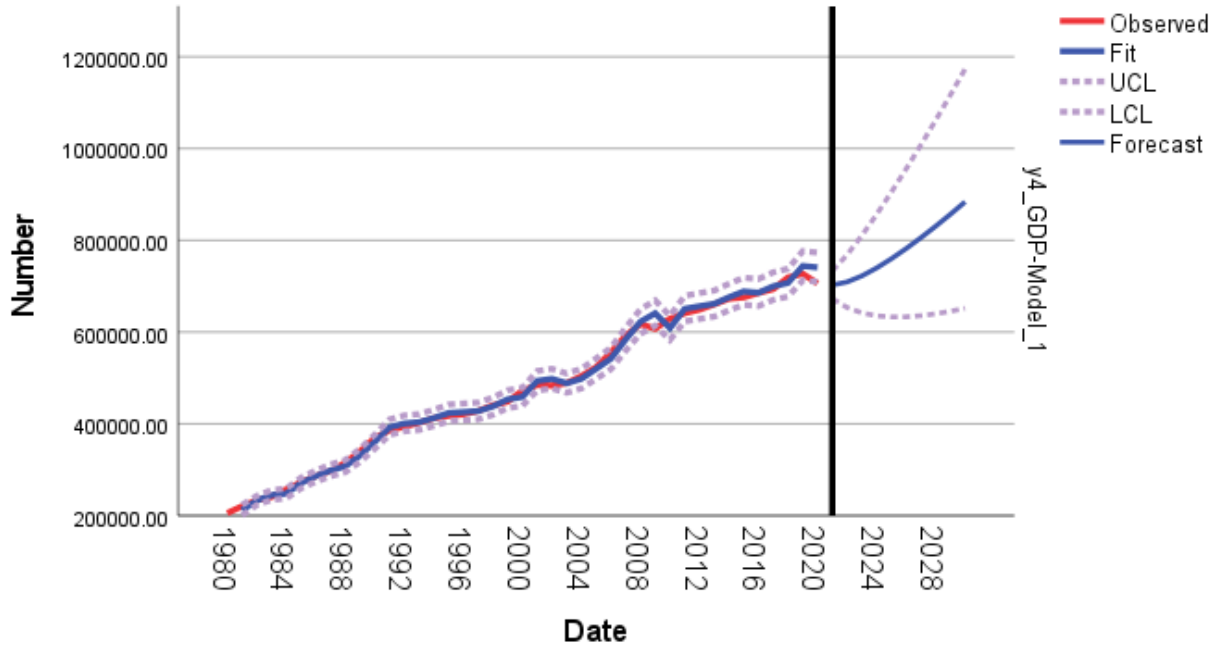


Figure 3-27: ARIMA Model with Forecast (GDP)

There is one last important remark on the use of ARIMA models. The values of the parameters for the selected model vary slightly depending on the software used for the calculations. The software being used for this dissertation are Eviews and SPSS. However, the p-values of the

parameters are almost identical between both software. Moreover, the forecasted values are also almost identical.

For defining the suitable model, Eviews is used because it gives a better outcome for comparison between models. While, for processing and forecasting the data, SPSS is used because of the efficiency of the software in terms of layout and better figures.

In the used example of GDP, the parameters for the Constant and AR according to Eviews are:

$c = 0.013101, AR(1) = 0.597796$

SPSS gave the results shown in Figure 3-28:

$c = 0.30\,, AR(1) = 0.598$

This slight difference makes no significant impact on the forecast.

ARIMA Model Parameters

				Estimate	SE	t	Sig.
GDP-Model_1	GDP	Natural Logarithm	Constant	.030	.008	3.711	<.001
			AR Lag 1	.598	.145	4.114	<.001
			Difference	1			

Figure 3-28: ARIMA Model Parameters SPSS (GDP)

3.3.4.2 Exponential Smoothing ETS

Figure 3-29 shows the Exponential Smoothing ETS forecasting method to forecast the Swiss GDP.

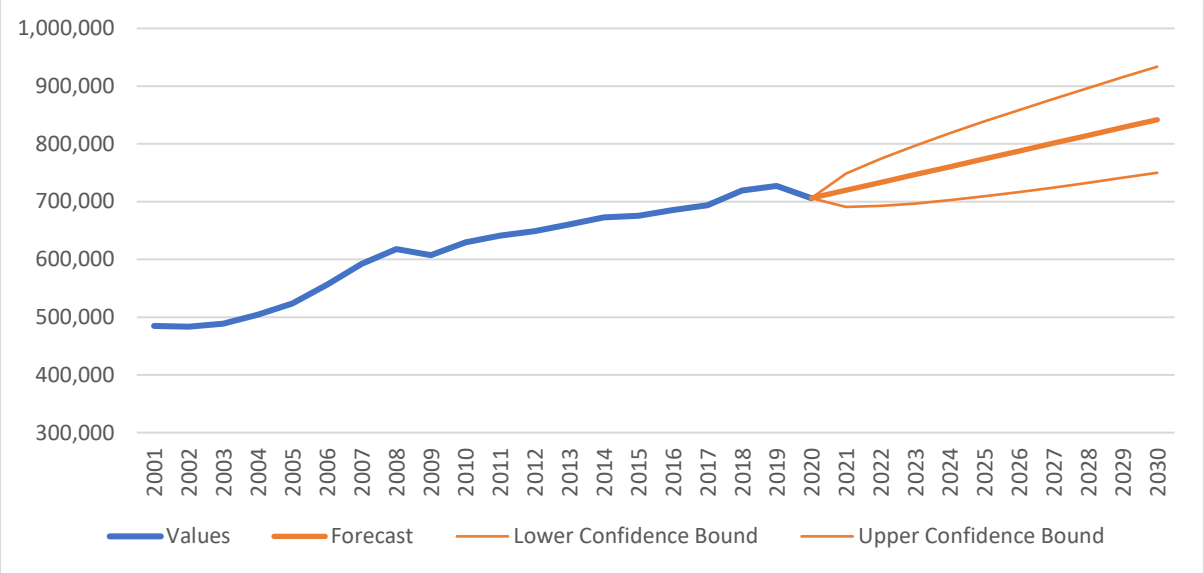


Figure 3-29: Forecasting GDP using Exponential Smoothing ETS

The forecast shows that the GDP will continue to grow in Switzerland in the near future.

The forecast values are presented together with the upper and lower bounds in Table 3.12.

Table 3.12: GDP Forecast Outcomes

Year	Forecast	Lower Bound	Upper Bound
2021	719,804	690,846	748,762
2022	733,366	692,434	774,299
2023	746,929	696,788	797,069
2024	760,491	702,575	818,407
2025	774,053	709,275	838,831
2026	787,615	716,623	858,607
2027	801,177	724,463	877,892
2028	814,740	732,690	896,789
2029	828,302	741,234	915,370
2030	841,864	750,043	933,685

Figure 3-30 below is to see how the two methods compare.

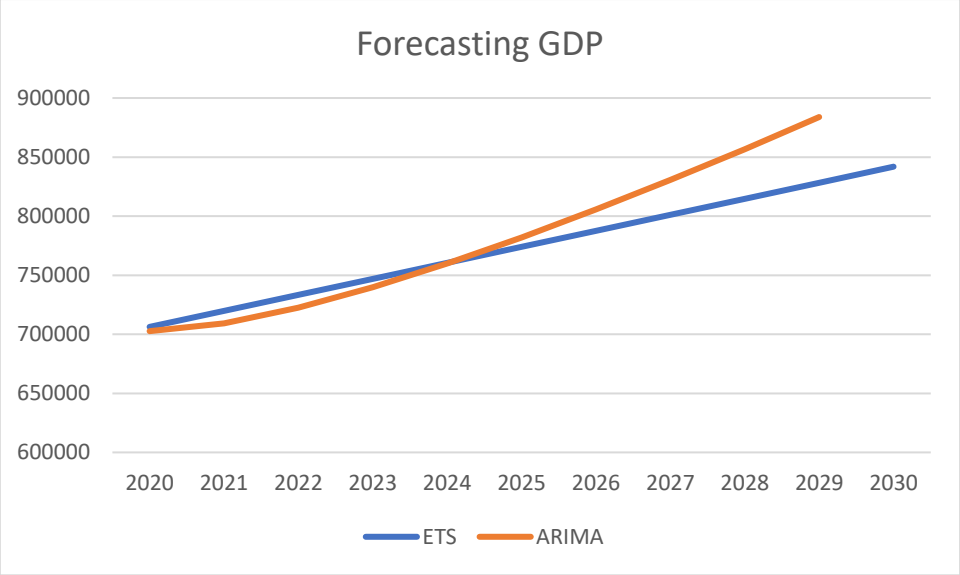


Figure 3-30: Forecast Methods Comparison

There is no significant difference for the first few years of the forecast. Later, ARIMA is a rather optimistic method than the Exponential Smoothing ETS.

The complete forecast is in appendix 7.2. In the next section, the presentation of the results is provided.

3.3.5 Summary of the Observation and the Limitations of the Forecast

This subchapter will summarize the forecast outcome in addition to the limitations of the selected forecasting models.

3.3.5.1 Results Summary

The summary of the forecast for all the variables is listed in Table 3.13.

To complete the analysis and the discussion of the outcomes of the forecast methods for all 23 dependent variables, we come to this conclusion. There will be in the future some decent prosperity for the society in terms of GDP growth for the country and growth in the gross national income (GNI) per capita, which yields salary raise for the society collectively. The economy will remain stable with improved exports and reduced imports of ICT products. The job market will not face a job-reduction tsunami due to technology. Despite creating many jobs in different sectors, basically in the healthcare and ICT sectors, unemployment rates will not drop significantly.

Table 3.13: Forecast Summary for all Variables

Variable	Description	Future trends	
		ARIMA	ETS
Y1	Investments in ICT in millions of CHF	++	+
Y2	Gross Capital Formation in million CHF (current)	N/A	+
Y3	GDP Switzerland in million CHF (current)	++	+
Y4	Gross National Income (GNI) per capita in CHF	N/A	+
Y5	Healthcare Costs in millions of CHF	N/A	++
Y6	ICT goods imports (% total goods imports)	N/A	+
Y7	ICT service exports in millions of USD	N/A	++
Y8	Medium and high-tech exports (% manufactured exports)	N/A	+
Y9	New businesses registered (number)	++	+
Y10	Number of SMEs	N/A	+
Y11	Inflation	N/A	+
Y12	Labor Force Participation in the Labor market	N/A	+
Y13	Unemployment, total (% of the total labor force)	N/A	+
Y14	Unemployment, male (% of the male labor force)	N/A	+
Y15	Unemployment, female (% of the female labor force)	-	+
Y16	Unemployment with basic education	-	- then +
Y17	Unemployment with advanced education	N/A	+
Y18	Employees in the retail sector	N/A	-
Y19	Male employees in the retail sector	N/A	-
Y20	Female employees in the retail sector	N/A	-
Y21	workers in the healthcare and social sector	N/A	+
Y22	Nurses and midwives (per 1,000 people)	N/A	+
Y23	Employment in agriculture (% of total employment)	N/A	-
Y24	Employment in industry (% of total employment)	N/A	-
Y25	Employment in services (% of total employment)	N/A	+
Legend:	- decrease + increase ++ massive increase N/A not applicable		

A higher proportion of the available labor force will be utilized in terms of percentage of employment (full-time). However, there will be additional training costs to adapt to the latest technologies in every sector, which might lead to higher employment costs.

The downside of the future trend is exemplified in the loss of jobs in the retail sector, but this (according to the forecast) is not related directly to applying technologies but rather to changing purchasing behavior trends with more people opting for online shops pushed by the Covid-19 pandemic.

A further drawback of the future society will be that salary gaps between the social classes will increase. The salaries will indeed improve in the future but not for everyone. The salary raise will be for society collectively, meaning that employees in the ICT sector, for instance, will get much higher pay than those in other sectors such as healthcare and services. The lower-class workers will struggle with more competition to find jobs as more people are forced to switch to the less-paying sectors. In addition to the struggle with fewer jobs and lower salaries comes the knock-out of increasing living costs (due to rising inflation) and growing healthcare costs which will make a serious intervention by the state vital. The government will need to reconsider a minimum wage for every citizen in society regardless of their employment status. The solution of an unconditional basic income could mitigate these negative consequences of technology and societal advancement. There has been a big debate on basic income, with strong arguments for and against the matter. The vote on June 5, 2016, when Swiss voters denied the initiative "For an unconditional basic income," should come again to question. In 2016, technology was not as advanced and implemented as it is today. Many jobs started partially to disappear. Therefore, the initiative of unconditional income must be discussed again and brought to the front by the state and society.

The well-being of individuals and life quality in the future smart society in Switzerland will most likely not enrich in the light of the technological revolution. However, countless social attributes cannot be forecasted, and humans have always shown a strong capability of adaptation and making do.

Many methods were tried for the forecast, and the most suitable was the easiest to apply ETS. ARIMA is a great forecasting method that was suitable for several variables. But many variables were non-ARIMA in nature.

Answers to research question

Like chapter 2, this chapter provides a detailed analysis which is part of the answer to research question number 2 (see Box 1-1 and Table 1.1) from a different perspective:

> How will the future society impact the lives of individuals? How will technology affect various aspects of life?

The summary of the answer is in Box 3-3:

Box 3-3: Answer to Research Question 2 (part 2)

More investments will be ICT sector which means creating both challenges and chances for people to adapt. The advantages will be in the form of improving lifestyle and easing difficult tasks. But the challenges will be with coping with all the technologies and not falling behind. Investments in infrastructure and education will continue which reflects positively on the people. The GDP of Switzerland will grow steadily thanks to its advancements in digitalization and innovation.

National income will continue to prosper and maintain the richness of Swiss people, but this has a bit little value for individuals because not every segment of people will benefit. This will come at the expense of people like employees in retail and similar occupations that can be replaced with machines.

Healthcare costs will increase especially with the current deficit between offer and demand for the healthcare sector (little offer). More people aging means more forces are required for nursing. People with lower income will suffer most from the increased general costs, which should ring a bell for the government to intervene and consider repairing the health insurance system.

Switzerland will improve its ICT goods and services exports and medium and high-tech exports which results in strengthening its position globally. This puts more pressure on people to pursue better education and might cause disturbance to the job market because higher qualified jobs might not find the right match in the local market. That issue is solved by acquiring foreigners (not necessarily bad) but will put more pressure on society.

The number of SMEs will continue to grow which is vital for the Swiss economy as it depends massively on it. This means that the Swiss economy will remain solid and keep providing

opportunities at least for the foreseen future. But this might increase social division, especially since inflation will continue to increase. The salaries do not increase at equal rates for all sectors of course, so inflation will hurt those with lower income (typically those jobs do not see significant salary raise).

The labor market will remain stable with more jobs created than deleted. This might be the case for a decade only, as globally the situation is reversed. The matter of economic transition and labor market shifts should not be overestimated. Jobs will be lost in some sectors and created in others, and people will adapt naturally as they always have. The aim here is to pave the way for adaptation and not shock society. The bottom line here is that people do not need to fear for their future jobs, but rather work together with the government on improving themselves and preparing gradually for the future.

Unemployment rates will not witness a sudden change other than steady numbers. People with basic education will have higher unemployment rates than those with higher education. Employees in the retail sector will face difficulties finding jobs in the next ten years, the opposite of workers in the healthcare sector. Nevertheless, nurses have low incomes and hard work environments. Intervention is needed so they do not pay an unfair price as they did during the Covid-19 pandemic.

The economy is shifting more towards services and away from agriculture and industry. This should be worrying for society as the dependence on importing food will increase, and small businesses in this sector will disappear.

The general observation and summary of the analysis suggest that the quality of life will not improve, and people will not be happier or healthier just because society is becoming smart. New problems will evolve in the future, and the small ones, for now, will grow. The future is not as promising as promoted.

3.3.5.2 Forecast Limitations

The independent variable "investments in ICT" alone is not accurate enough to represent the technological advances in society. It is just an indicator of the importance of technology to society. It also provides a limited representation of the technological state in society. One should also bear in mind that not every franc invested in technology yields gain for society.

Additionally, even if another independent variable is defined and supposedly the historic data sets are available as they are needed for the forecast, the technicality of the forecast gets much more complex. It needs advanced skills in statistical methods and programming because the task will analyze the impact of two independent variables on several dependent variables simultaneously. However, the real limitation here will be the low number of observations which is approximately 20 observations.

Another issue is the interconnectivity of some dependent variables, such as the variables related to the job market. Analyzing the potential relationship between these variables and the interaction between them and the independent variables would be appealing research for future research. However, this is out of the scope of this dissertation.

There are hidden factors that contribute to the direction of a variable, whether it increases or decreases in the future. These cannot be easily spotted because of the complexity of the society's economy, and even some factors are identified; it is almost impossible to represent them in historic data sets that match this forecast's design.

Some variables face limitations due to the nature of these variables and not the forecasting method. These are the variables that are related to the three-segment economic model.

The limitation of the Pearson Correlation Coefficient (PCC) is that it only indicates the correlation and not the causation. Therefore, the R-squared value helps better understand the relationship between the two variables and the percentage of the variances explained by correlation.

VAR models have certain weaknesses because they do not describe or contain the economic structure (Trenca et al. 2011) when applied. For the case of forecasting, this limitation is less significant, but it is still somehow relevant when the purpose of the forecast is to determine the causal relationships between the macroeconomic variables.

Despite the Exponential Smoothing ETS model is simple and easy to understand, its main limitation is that it neglects to account for dynamic changes in the real world and is based too strongly on historic data. Additionally, as it was noticed in the forecast, this model sometimes fails to handle trends well, which results in inaccurate outcomes. Nevertheless, the forecast was a success, and it delivered all the necessary outputs to serve the purpose of this dissertation.

After talking about enough concerns about the future from every possible perspective, it is time to act and try to secure the future. The next chapter which is the core contribution of the dissertation will recommend a solution to preserve society and restore leadership to the favor of the people.

4 Smart Sovereignty: Security Concept for Society 5.0

All previous chapters have contributed to the preface of this chapter of the dissertation. Chapter 2.1.5 introduced Society 5.0 as a normal social transition and discussed its technologies. Chapter 2.2 explored the definitions of security and introduced a modern definition of "Societal Security" in chapter 2.2.2 which comes to use in this chapter. Chapter 3 presented most types of risks that Society 5.0 needs to prepare for as the many diverse threats which accompany technology could hit future society hard.

Now, that all pieces are complete, it is time to introduce a novel concept called "Smart Sovereignty" to shield our security as humans against the relentless, overwhelming waves of technologies and robotics. Smart Sovereignty will prepare society for a smooth transition to Society 5.0. This chapter is the most important contribution of this dissertation. It also answers the third research question (see Box 1-1 and Table 1.1).

> What is the sustainable solution which reduces or negates the negative effects that accompany technology?

Figure 4-1 presents the outlook of this chapter.

Figure 4-1: Chapter 4, Outlook

Society is faced with the dilemma of having to choose between pushing towards more digitalization and profiting from the advantages of Society 5.0, and backing off a little bit and keeping safe from the threats that come with it. Unfortunately, the choice is not for the people to make. The interaction with other nations pushes the local society in a certain direction. The only solution would start by acknowledging the problem and being aware of the dangers, and preparing with the right equipment. Ideally, society will be in great shape if people become sovereign themselves. However, that will not be possible without building trust. The element of trust is extremely vital for the society for a service to remain in use. It is necessary to examine digital trust and digital ethics because of their significance for the smart society.

Technological advancement could be a great improvement and bring prosperity to our societies, although this requires thoughtful and accountable utilization of the tools equally at the individual level and the level of society. The present worry is that the foreseeable future does not seem very encouraging if these risks and threats, which already have generated significant problems, have not been addressed correctly, particularly when considering that they will be gradually more complex. There is an unequivocal and urgent need to introduce a new concept that will enable people to re-establish their sovereignty and take over control, thereby maintaining and safeguarding human society from becoming destroyed by technology.

After presenting the challenges and possible problems that are associated with technology for the 4IR and Society 5.0 in chapter 3, and together with this introduction to show the need for real sovereignty to grant an alleviated society, the aim now is to suggest useful measures and actions which are compulsory to sufficiently confront and appropriately respond to the risks. Regrettably, the solution is neither simple nor straightforward because the problem itself is extremely complex to understand. Nevertheless, some things can be made as a primary action to decrease the potential damage and slow down the downsides of the technology.

Governments are responsible for working on a wide range of societal pillars like education, economic growth, environment protection, industry backing, defining all necessary stakeholders, getting them involved in planning, assuring transparency, and putting the public's interest first. Since there will always be conflict and clash of interests between stakeholders, it is imperative to guarantee careful planning, righteous priorities, and unbiased responses when disputes happen. It is important to hold politicians, unions, social activists, and government officials accountable and liable for their actions and motivations. There is also a

need to restructure and improve the education system to include a wider range of disciplines and necessary future IT knowledge.

There is a general need for a new approach to monitoring and controlling the security pathway in modern societies. One fundamental measure that should be taken is assuring an acceptable level of protection for the data that is the foundation of a smart society. Similarly, protecting the information and physical assets. The aim is to efficiently reduce the negative implications of the mass-dependent on technology without eliminating the countless benefits and quality improvements that a smart society carries for the population. Nevertheless, people should be able to supervise, be informed, and be aware of crucial decisions taken by authorities and responsible parties, and people should be able to intervene in vital conditions and veto irrational choices and decisions that are not in the public favor.

Individuals cannot deal with these duties and such big obligations when separated. Therefore, these responsibilities require the collective efforts of united persons. Moreover, people will need proper related education and perhaps specific workshops to form the important basic knowledge and become capable of making decisions.

The solution could start with forming a body that works similarly to a union in terms of organization, communication, structure, clear responsibilities, task distribution, transparency, and goals. The core goal of this body is assuring that people become the real sovereigns and have a say over their data and privacy, decisions that shape their future, the right to know and be aware of possible hazards that come together with technology, and finally, putting the interest of the public and the society above the interest of big corporation and politicians. This chapter presents the solution as a new concept that shall be named “Smart Sovereignty”. The rest of this chapter offers a comprehensive explanation of the smart sovereignty concept and presents the historic background for sovereignty and how the interdisciplinary term often used in politics can be implemented in smart societies. In addition, this chapter intends to explain how smart sovereignty is expected to operate in smart society and how to be measured and improved over time to grant its success in restoring power to people and limit the downsides and the negative effects of technology on technology the future human society.

One big concern in politics related to achieving smart sovereignty in Europe is governmental surveillance. For many years, China had many conflicts with leading western corporations such as Google, Microsoft, and many others resulting in denying their services in China. Attention

should be drawn to the problem of Internet sovereignty in the shadow of such conflicts under authoritarian regimes like China, Russia, Iran, and many other countries. Beijing has succeeded in obtaining people's compliance and following strict regulations. Despite public challenges, Beijing could also reinforce its political rule (Jiang 2010). Later, China's Internet surveillance strategies resumed showing an Internet evolution and governing model - authoritarian informationalism – which blends the components of capitalism, authoritarianism, and Confucianism (Jiang 2010). Unfortunately, data collection about people's privacy will only increase because of the augmentation in the number of used sensors and applications that enable the government to trace down people's activities, detect their behavior, and increase spying (Caron et al. 2016). Contrariwise, the IoT literature suggests that people are prepared to provide some of their personal information and a portion of their privacy in cases where they trust the technology service providers and when they see that the service is valuable and useful (Culnan and Armstrong 1999).

Additionally, they have no other option in countries like China and Russia. Despite many years passing after the Soviet Union lost the Cold War, Russia is still modern, namely information war against the liberal democratic system of western Europe and the United States. Russia seems to be desperate to achieve victory in this war. Internet governance, cyber security, and surveillance of the media are not treated separately in Russia, as they are all part of the information security that shapes the foreign policy of Russia. The coming years will bring increased importance to geopolitics in the information domain and carry more challenges to Europe (Maréchal 2017). These practices of China and Russia challenge the concepts of privacy and security and threaten the prosperity of smart societies in the form of challenging the freedom of speech and hindering digital human rights.

In the contemporary age, direct intervention in other countries' internal affairs is not seen as acceptable officially, except for the countless times the United States, France, and China interfere and often with military forces, as the interference puts the country's sovereignty in jeopardy. Nevertheless, there remains a possibility to push for a transformation in another nation without menacing its sovereignty by combining diplomatic and political pressure, international conventions, and treaties.

The G20 countries and the rest of the advanced countries like Switzerland and the Nordic countries may well and ought to adopt inclusive methods to raise digital-industrial innovations

for better job creation and sustainable economic growth. The world will need to reform packages on every level of society and industry. The reform should be accompanied by initiatives to restore balance for demand and supply of skill sets, labor market reforms, reshaped social security networks, actions to endorse digital innovation, enable the implementation of sophisticated technologies, and support private and public sectors training and educational programs.

Sovereignty in action

Here are two good examples of what sovereignty looks like when put into action. The first is a tendency that appeared as a natural reaction to the decision of WhatsApp to transfer the data of its users to Facebook (Lanxon, 2021). Luckily, people got well alerted and became aware and started what can be called massive migration from this app to a competitive app called Signal (as suggested by a tweet by Elon Musk) with hopes that this would break some of the control of WhatsApp and Facebook. The positive thing here is that people, when well-alerted, are ready to take measures and make the right decision to retain their sovereignty.

The second example is the ongoing clash between Google and Facebook from one side as a source of news, against the Australian government and the classic news networks, and the traditional media over advertisement revenue and other matters (Hart, 2021). Google is now threatening to shut down its search engine in Australia. The positive thing here is that governments started to seriously challenge big corporations like Google, which is the right step in the direction of sovereignty.

4.1 The Origins of Sovereignty

This subchapter discusses the origins of the term “Sovereignty”, where it started, and how it was used and developed throughout history up to the point where it is put in a digital context for the protection of smart societies. The reader who is familiar with this field of politics or who is not interested in the political background can skip immediately to Figure 4-3 which provides a summary of the timeline of sovereignty, and read from there on.

Why it is important to look at the history of the definition and the meaning of sovereignty

The dominant story broadly spread about sovereignty is the conventional theory about sovereignty supported by the leading scholars in International Relations (IR). IR scholars believe that the traditional rights of states which implies the right to freedom from interference as the necessary and timeless essence of sovereignty.

Literature in International Relations tells the story of traditional sovereignty as it is initially founded at some point around the seventeenth century. Traditional sovereignty is often referred to as Westphalian sovereignty. Its initial meaning did not see adjustments or different conceptualizations for the coming centuries afterward (Glanville 2013). The traditional concept of sovereignty meant that governing bodies, countries, states, and kingdoms owned the right to rule and govern themselves as they see fit without external interference or intervention. Over the last few decades, the traditional concept of sovereigns has been disputed by conceptions of restricted and accountable sovereignty. As told by IR, this story is widespread and agreed upon by many researchers even though it carries risky concepts like “license to kill” (Glanville 2013). Since the early seventeenth century, states believed that they – as sovereigns - own the privilege to kill, murder, displace massive numbers of people, and even make genocides without anyone intervening in their actions as long as it is done on their soil (Evans 2008). It is important to note that the “traditional” meaning of sovereignty was only resolutely founded by the society of states and IR scholars in the twentieth century when political scientists dedicated little consideration to sovereignty during the 1960s and 1970s and not before (Glanville 2013).

However, limiting and simplifying the history of sovereignty to this extent and accepting that sovereignty is so fundamental and enduring is a mistake because any historical evidence does not support these claims, as Glanville (Glanville 2013) argues. During many centuries of sovereignty, there has been an understanding that the core characteristic of sovereignty includes the right to wage war and only fair and just wars in addition to intervening in other states' affairs. These characteristics have evolved and changed over time, and it was true for a certain time that states were convinced of the rights that the “traditional” sovereignty granted them, which is the freedom from outside intervention (Glanville 2013).

The lasting conventional story of sovereignty claims that the historical origin of sovereignty started in 1648 when the states earned their right of noninterference after the Peace of Westphalia. This right came under question after the emergence of humanitarian intervention

during the cold war (Philpott 2001). However, Philpott claims that the past three hundred years did not see any noteworthy change in the meaning of sovereignty (Glanville 2013). In the past four centuries, two major historical events have resulted in reshaping the organization of the world and granting states recognized and organized right as sovereigns. This was the Peace of Westphalia in 1648 after the Protestant Reformation, which finished medieval Christendom and created a system of sovereign states in Europe. The second was the ending of colonial empires around 1960, caused by the notions of equality and nationalism, consequently expanding the sovereign states' regimes to the rest of the world (Philpott 2001).

Most scholars in various international relations schools present a state's sovereignty as timeless and objective, whether on purpose or not. By doing so, they promote sovereignty to be static and non-changing throughout the history of its existence. Even English language scholars who study the historical changes in notions concerning societies derive definitions. They tend to give sovereignty a static terminology involving a right of nonintervention (Glanville 2013). In Realism -one of the most dominating schools in international relations- scholars tended to focus little on the history of sovereignty and its nature. As an alternative, they treated sovereignty as an experimentally quantifiable characteristic of statehood. On the other hand, for several neo-realists, sovereignty is seen as a state's capability to take authoritative decisions (Glanville 2013). That was apparent in the writings of a famous realist critic, Waltz, who declared that a state is considered sovereign only when it can decide how it will handle its internal and external problems (Hast 2016).

Naturally, there have been some improvements and challenges to the concept of sovereignty, such as the static and historic nature. Also, several scholars had their own words and stressed points in defining the meaning of sovereignty. However, all these definitions and visions did not extend beyond the limited perspective of traditional sovereignty as adopted by mainstream IR literature. Here are a few examples of these varying interpretations of the sovereignty concept.

According to Gilpin, sovereignty status for a state reflects the nonexistence of superior authority to the state internationally (Gilpin 1981). He said, ‘‘The state is sovereign because it must answer to no higher authority in the international sphere. It alone defines and protects the rights of individuals and groups.’’ (Glanville 2013). A realist scholar Krasner implicitly argued that sovereignty has a static nature. He coupled sovereignty with Westphalia when he

noted that Westphalian sovereignty is the fundamental rule. By this rule, the state should be able to abstain from intervening in the internal affairs of other states (Krasner 1999). Hence, not only Krasner coupled sovereignty with Westphalia. As previously mentioned, traditional sovereignty is strongly connected to Westphalia in the traditional and conventional story of sovereignty.

Over the past few decades, important academics and thinkers have created new understandings of sovereignty's problematic definition and concept. They underlined its contingent and contested nature (Glanville 2013). Rather than stating that sovereignty is a natural and static notion, they came up with the idea that sovereignty is a practical category whose experimental elements are not static. However, it progresses in a manner that reflects the active, practical consensus among effective politicians, as Ashley declares (Ashley 1984). They concluded that sovereignty does not have an essential static significance. Rather, they found that sovereignty has a meaning that is given and designed socially and historically. Moreover, they noticed some important shifts in the structure of sovereignty compared to its initial emerging meaning – all according to the traditional theory – compared to how it developed in the twentieth century (Glanville 2013).

The development of other views on the origin of sovereignty which highlight its conditional and disputed nature has allowed scholars to clarify how traditional sovereignty changed in recent decades and went through two significant phases which formed these two main sovereignty concepts: traditional conditional sovereignty and responsible sovereignty. However, these two concepts uncritically assumed that the traditional concept of sovereignty existed since the seventeenth century and not earlier.

To summarize the important matters in this section so one can move on to the next segment, the adapted traditional history about the static meaning of sovereignty and its birthdate is not backed up by historical events, and it goes long further back in history. Its beginning belongs to the thirteenth century and carries the meaning of “the right to wage (just) war” (Glanville 2013). It did not carry by its airs the notion of the non-interference. Figure 4-2 summarizes the conventional story of sovereignty.

Figure 4-2: Conventional Story of Sovereignty

The early modern period around the thirteenth century saw the emergence of the sovereignty concept in Europe. It was first understood as the right to wage war. Only the real sovereign possessed this right: the prince alone. The prince had the right to wage just war, defend society, and punish criminals (Aquinas 2002). In the thirteenth century, Pope Innocent IV declared that he possessed the universal authority to punish violations of the law of nature (Glanville 2013). This declaration was a sign of the birth of the notion of sovereignty because this implication will be the cornerstone for the meaning of sovereignty in the coming years.

In 1621, Suarez, a priest, theologian, and philosopher, formulated the right to wage just war like sovereignty. He asserted that because there was no greater human authority on earth, the right to wage just war, punish criminals, and prevent injury in the community was in the hands of the sovereign prince (Glanville 2013). In the vision of Suarez, the world needed this kind of power.

A few years later, in 1625, Grotius - a Dutch jurist and one of the first to help lay the foundations of international law – wrote his book "The Rights of War and Peace". In his book, he extended

the rights of the sovereigns beyond only punishment between individuals and states. His idea was that the individuals in a community have the right to defend their lives and the right to punish who causes them injuries, and so do sovereigns. He declared that the sovereigns have the international right to defend themselves and prevent injuries from happening to their states, and additionally, they have the right to penalize serious violations of the laws of nature and the laws of the nations (Glanville 2013). With his strong and clear statements, Grotius put himself together with the Pope in the same rank and granted universal authority to the kings.

Grotius was committed to following the opinion of the innocent, punishing tyranny, and rescuing the oppressed (Glanville 2013) to make the war just (Tuck 2001). Furthermore, Grotius defined a variety of violations of the law of nature in which the sovereigns owned the right to punish and wage war. These violations included being inhuman to the parents, eating human flesh, killing strangers, and practicing piracy (Tuck 2001).

The vision of Grotius about sovereignty had a nature of the intervention. At the same time, common people had no right to rebel against tyranny or their law violations because of the absolute superiority of the sovereign, who enjoyed interfering in other sovereigns' affairs (Piirimäe 2011). Additionally, his sight on sovereignty did not match the ideal paradigm envisioned by the advocates and thinkers of Westphalian sovereignty. Grotius was a neo-scholastic in his vision of just war as a method of sentence for the breaches of the law of nature and universal morals (Piirimäe 2011). In Grotius's thinking, a just war means that there could be only one side who is just in war. This discriminatory idea is dangerous because it can cause much suffering in wars for innocent people. Therefore, Grotius suggested a distinction between formal and nonformal wars without abandoning the moral difference between the just and unjust sides of the war. This notion of differentiations became dominant in Europe in the seventeenth and eighteenth centuries (Piirimäe 2011). Europe gave the impression that it stood as one community ruled by universal morals built by natural law and was not supported by legal enforcement. Nevertheless, there have been alternative ways to impose universal norms, enhance the belonging to international public opinion, and promote the status of states and sovereigns (Piirimäe 2011).

By the mid-eighteenth century, writers and scholars started to form a more precise meaning of sovereignty and sovereign right that revolves around the notion of non-intervention (Glanville 2013). One of the most important scholars was Vattel, an international lawyer, and

writer of the book “The Law of Nations” in 1758. The influence of Vattel in this era encouraged some authors to name the non-intervention sovereignty model “Westphalian / Vattelian sovereignty” (Krasner). Vattel reiterated Grotius and others in preserving that the universal moral law remains valid to sovereign states in an international state of nature as it was to people. Vattel likewise asserted that universal moral laws should not be too strictly applied and put into force. Otherwise, states' natural freedom and independence will often be breached, and this will destroy the natural society of states (Glanville 2013). Vattel indicated that all states should be compelled to regard the liberty and the independence of each state as long as this state does not interfere with the freedom and the independence of other states. This suggestion holds even if the state used illegal and brutal actions within its territory (Glanville 2013). In the vision of Vattel, the right of non-interference is a natural phenomenon that accompanies the natural freedom and independence of nations.

Additionally, all nations should have the right to be ruled as they believe appropriate, and no country has the lowest right to intervene in the government of the other. Moreover, sovereignty is undoubtedly a nation's most important right, and other countries must carefully respect this right. These notions were so influential that they were used as arbitration (New York state. Legislature. Senate 1841) and tools to solve the conflict between the United States of America and Sweden over the case of the motorship “Kronprins Gustaf Adolf” and Pacific in 1930 (United Nations 2006).

To summarize, the conception of sovereignty in the era of the early modern period 1500 – 1800 AD and during the mid-thirteenth century revolved around the rights of the sovereign prince to wage war and to use the sword of war to protect the commonwealth against enemies. The absolute supremacy of the sovereign means that people had no right to resist tyrannical violations of the law of nature. No one prevented Sovereigns from intervening in each other’s affairs. They conceived the right of intervention as a necessary attribute of sovereignty (Glanville 2013).

Toward the nineteenth century, the meaning of sovereignty as the right of non-intervention grew progressively agreed upon by law theorists and legislators. There remained some tension between the 19th-century modern concept of sovereignty and the alternative interventional notions of legitimate sovereign law. The Western European countries understood that the excessive use of power in the name of sovereignty could lead to international disorder. The

French Revolution and the wars that Napoleon carried out afterward clearly demonstrated this risk. These concerns were addressed in the Vienna Congress in 1815 when some European countries pledged to use force to safeguard the recently proclaimed legitim principle of rulers in monarchies. The aim was to preserve stability in Europe (Glanville 2013). Austria, Russia, and Prussia formed an alliance called the Holy Alliance, which developed a new right of interference to stop or beat any uprising revolution by people all over Europe. The alliance considered any revolution illegal and a means of causing political instability.

Additionally, cruel intervention to suppress rebellions is both permitted and mandatory to protect the international order (Finnemore 2003). The new rights of intervention were clearly stated in the words of von Metternich, the Austrian Chancellor, between 1821 and 1848, when the liberal revolution forced his resignation. Von Metternich claimed that once a government cannot perform its duties and obligations towards international treaties due to domestic social chaos, then this government and other neighboring governments have the right to intervene, suppress, and prevent any revolution (Heraclides and Dialla 2016). He further compared this situation to a case where any person must put off the fire in his neighbor's house before the fire spreads to his house (Barkin and Cronin 1994). In connection with these statements and legislations, the Austrian, Russian, and Prussian Holy Alliance carried out several interventions in 1820–1821 to halt revolutionary movements and backed up the threatened monarchs in Naples, Piedmont, and Spain (Glanville 2013).

Another attribute of legalizing intervention apart from political and social stability was humanitarian intervention. So, the sovereign's rights to non-intervention became challenged with a new exception.

The right of the sovereigns was not looked at entirely and unconditionally as the right of non-intervention. It was surrounded by several exceptions and means to be violated justifiably. The legal power of sovereign rights was limited, contrary to the fundamental rights of the sovereigns, creating a paradox. The focus on liberty, independence, and the right of self-defense owned solely by the sovereign has steered many scholars to deny that countries' interventions in each other’s internal issues should be judged. Vattel, for instance, was amongst those who asserted that it is only up to the state to decide the occasions in which they can justifiably intervene in the affairs of others, even to the limit of invasion or conquest (Glanville 2013). Therefore, it would be wrong to assume that the traditional meaning of

sovereignty was only the right of non-interference, especially when we know that till the 19th century, the discrepancy between intervention and war was not completely cleared out (Chesterman 2001).

Right after World War I, the international society made important moves to ascertain the rights of the sovereigns of non-intervention. Nonetheless, only by 1945, the international society made the traditional meaning of sovereignty stable and unambiguous (Glanville 2013). The cold war will later have many implications and bring more challenges to the sovereignty concept, and the traditional meaning of sovereignty will be replaced with a new concept that revolves around conditional freedom from external interference. Sovereignty after the cold war also means obligations for the states, including protecting human rights by preventing wars and supporting self-determination (Conlon 2004).

The post-Cold War era witnessed general approval that countries are accountable to the international society in protecting their people. Sovereignty has ceased to be a cover for international monitoring, denunciation, imposition of sanctions, or a means to intervene with armed forces (Glanville 2013). The member states of the UN announced that they are responsible for protecting their people from genocide, war crimes, ethnic purification, and crimes against humanity and that the countries are willing to take the necessary actions if a country fails to perform its responsibility (United Nations 2005). Later during the Libyan revolution in 2011, the Security Council appealed against the responsibility to protect and permitted the usage of all the necessary actions to safeguard civilians from the threat of genocide and massacres in the sovereign state of Libya (Glanville 2013). That clearly showed the different understanding of sovereignty from how states and thinkers perceived it during the Cold War era.

Nonetheless, sovereignty today remains close to the traditional meaning that implies the right to freedom in addition to the responsibility to protect. The reality is sadly far away from political debates and official statements. Using power to enforce sovereignty brought the world many miseries. Sovereignty is supposed to defend human rights and human lives. The misuse of the concept by downplaying the obligations and the responsibilities of neighboring states, either by intervention or non-intervention, allowed military interferences that caused massacres, genocides, and ethnic cleansing. The international society often overlooked countries like Somalia, Haiti, Bosnia (Conlon 2004), and Syria. Some advocates held the concept

of sovereignty responsible for the miseries of humanity throughout history. They adopt an idealistic vision that suggests a new reframing for sovereignty in a way it can succeed in put an end to violence for good (Glanville 2013). However, in reality, sovereignty is more complex, but what Evans says remains true "Prevention is the single most important dimension of the responsibility to protect" (Evans 2008). Figure 4-3 presents the timeline of definitions and understanding of the meaning of sovereignty throughout its history.

Furthermore, it is right to believe that the advancement of sovereignty was not linear over the centuries (Aldabbas et al. 2020a). An important attribute and characteristic of sovereignty were its center. Sovereignty has often shifted between emphasizing a state-centric from one side and a people-centric approach on the other side. In international relations literature, sovereignty had two diverse natures of entities: state sovereignty and national sovereignty (Grotenhuis 2016). State sovereignty is specified and bordered by the territories where the state has its authority and legitimate rule, while national sovereignty is defined by people's sense of belonging to a certain race or their sentimental belonging to a community (Grotenhuis 2016). These two opposing sovereignty approaches caused political science debates in the past century. Some scholars (Barkin and Cronin 1994) observed that a state-centric method of sovereignty became dominant after the Napoleonic wars. However, nation-centric sovereignty became dominant after the first World War. Later, after World War II, state-centric sovereignty gained popularity and dominated that era. The post-Cold war era made nation-centric sovereignty dominant in most parts of the world (Grotenhuis 2016). The sovereignty notion subsequently developed to be a concept of the Nation-State. Sovereignty gives the legitimacy and authority to the state to rule as it wishes within its territory and is also the means for the states to communicate and interact with each other (Aldabbas et al. 2020a).

A nation-state, by definition (UNESCO 2017; Grotenhuis 2016), is a sovereign state with geographical territories where the subjects or the majority of them share the same culture, enjoy a common identity, and are organized in a political body.

Pope Innocent IV claimed universal authority for the punishment of violations of the law of nature

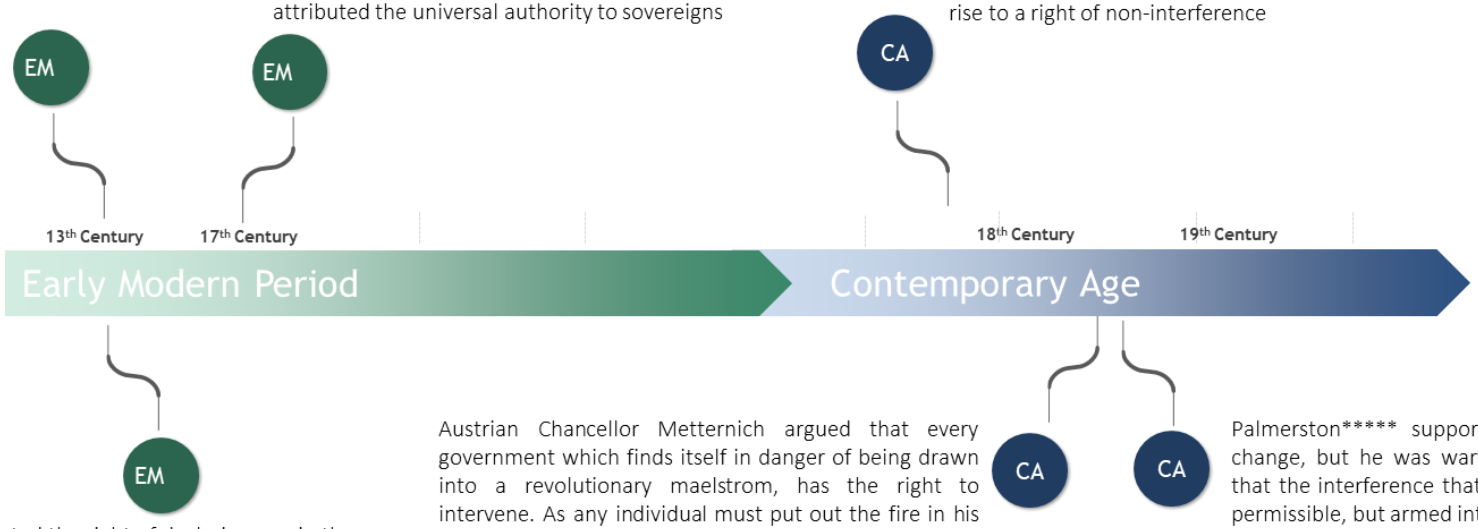
The establishment of the right of the sovereign prince to wage war. Aquinas* instated that only the prince has the right to wage war

Grotius** wrote "The Rights of War and Peace" where he defended the right of just punishment in an analogy between natural individuals and states. Individuals enjoy the right to defend their lives and the right of chastisement, as did the sovereigns in an international condition of nature

Grotius aligned himself with Pope Innocent IV, and attributed the universal authority to sovereigns

Clear statements of a sovereign rights of non-interference first appeared in the mid 18th century in the writings of Wolf*** and de Vattel****

Vattel maintained that the natural law is applicable to sovereign states in an international state of nature, just as it is for individuals. For him, the natural liberty and independence of states gave rise to a right of non-interference



Suárez* articulated the right of declaring war in the language of sovereignty. In the absence of supreme earthly authority, the right of just war or just punishment rest in the hands of sovereign prince

Austrian Chancellor Metternich argued that every government which finds itself in danger of being drawn into a revolutionary maelstrom, has the right to intervene. As any individual must put out the fire in his neighbor's house if it is not to spread to his own

On the grounds of Metternich, the Holy Alliance undertook interventions to stop revolutionary movements in the monarchs of Naples, Piedmont and Spain

Palmerston***** supported the liberal movements for change, but he was wary of intervention, so he insisted that the interference that consisted of friendly advice was permissible, but armed intervention was not

Palmerston declared that every nation has the right to manage its own internal affairs as it pleases, so long as it injures not its neighbors

The new principle of non-intervention was grounded in an emerging principle of national self-government. The sovereign right of non-intervention became accepted by some states as a reflection of the liberty of nations to govern themselves

* Priest, philosopher and theologian
** Dutch jurist, his works (in addition to others) laid the foundations of international law
*** German philosopher
**** International lawyer, wrote "the Law of Nations"
***** British Prime Minister

Figure 4-3: Sovereignty Timeline

Traditionally, the sovereign nation-states' interaction with one another under non-intervention treaties is organized systematically and adheres to international treaties, international organizations, international agreements, and global human rights, and is often monitored by the global community. The means and channels of communication are largely operated and monitored by the official heads of the state. Enterprises and companies exchange products and information through these channels. The only possibility was for the subjects in each state to communicate with one another through the same channels. Figure 4-4 shows the classical interaction between sovereign states and their elements (Aldabbas et al. 2020a).

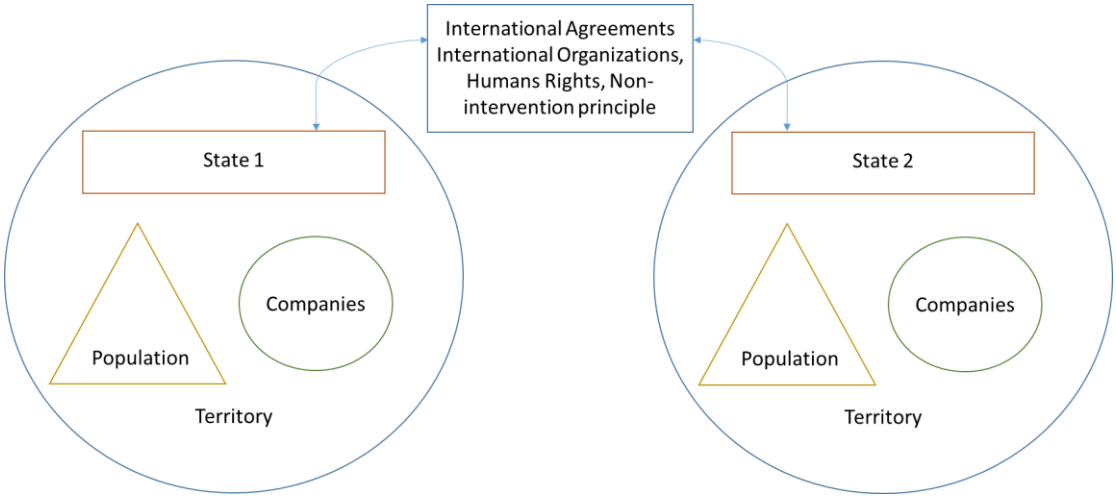


Figure 4-4: Traditional Sovereign States Interaction (Aldabbas et al. 2020a)

In the past few decades, augmented changes in international communications resulted in increased availability of direct connections across borders and exchanged influence powers between influential entities in several nation-states. Consequently, this has challenged sovereignty as we know it in the post-Cold War era. A more sophisticated communication diagram is easily spotted in the modern world as enterprises and corporates in one state can communicate with their target audience and customers in another state. Products, services, concepts, lifestyles, and political and social movements are being transported, sold, spread, and shipped universally without going through the inferior traditional state-controlled and monitored channels. Figure 4-5 illustrates a fictive example of components in state A communicating and spreading in state B. The more dominant state entities spread to weaker states to affect their population and culture and promote their goals. The weaker receiving state attempts to reduce these effects and limit the changes as they can threaten its sovereignty by setting entry barriers, but it can never be sufficiently successful. Nevertheless,

the sovereignty of state B is being severely contested. Hence, despite that the barriers in the Figure 4-5 are supposed to deny the exchange between states, they only can limit it.

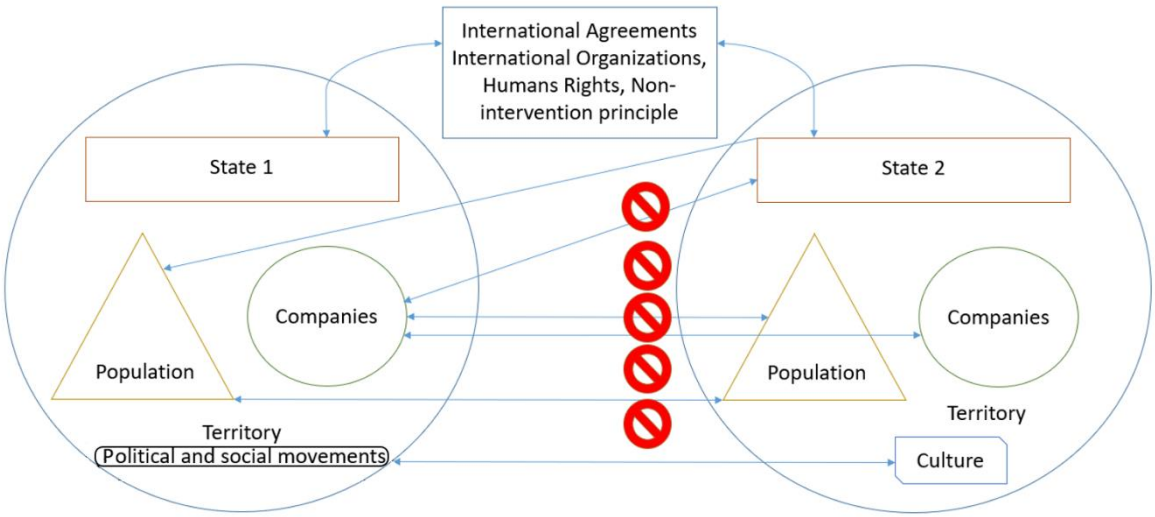


Figure 4-5: Modern Sovereign States Interaction

We are about to enter a new era of sovereignty, the post-digital revolution sovereignty. Sovereignty is becoming tougher to preserve, trickier to define, and more complex to determine its nature. Is the nature of sovereignty still nation-centric? Or did it swing again to be state-centric? Are we witnessing a new individual-centric, or rather something novel? These questions are difficult to answer. However, what is certain is that the world needs a new concept and modern understanding of sovereignty, namely, smart sovereignty.

4.2 Definition of Smart Sovereignty

To define smart sovereignty, one should start from the original meaning of sovereignty itself, as has been comprehensively investigated. In a democratic social system, the state should guarantee, to the extent possible, the self-determination of individual citizens. If this legal self-determination of the individual is established and guaranteed in the state polity, the individual can also be described as legally sovereign in that respect (Gräf et al. 2018).

There has been a widespread debate about Europe's digital sovereignty. This debate broke out in 2013 due to Edward Snowden's revelations of the secret US-NSA program, PRISM. The program was mass surveillance of the communication and emails of countless governments, businesses, and civilians, plus alliances of the United States in Europe and Latin America (Bauman et al. 2014). Triggered by issues like the US being up against the rest of the world and

the need to choose between surveillance and privacy, digital sovereignty evolved to be a buzzword in the digitization policy. It appeared in agreements such as “technological sovereignty” on the agendas of the German government (Gräf et al. 2018).

Who has the potential to be sovereign, and what are the circumstances to achieve this sovereignty? What are the greatest challenges to reaching smart sovereignty nowadays?

The main principle of smart sovereignty addresses individuals and normal citizens and aims to make them the real sovereign in their societies as technology users or citizens of the country. Smart sovereignty can be applied to countries whether they have national-centric or state-centric nature. It can also be applied to associations and organizations of these states. Smart sovereignty includes the notion of the right to informational self-determination, which is the most important aspect of smart sovereignty. That also reflects the right of individuals to decide for themselves on the disclosure and the use of their private data, in addition to the ability to use digital technologies according to their perspectives and perceptions.

Smart Sovereignty is a visionary concept that aims to guarantee and uphold societal security, but it is more specific as digital rights or data protection. This chapter will attempt to describe what this precise concept covers and how it can and should be used to reach an optimal and peaceful digital society.

Smart Sovereignty's purpose is to establish a roadmap to lead society toward a more secure environment in the context of the above-described factors. To achieve Smart Sovereignty, the idea and definition of various technologies need evaluation and updating. The meaning and goal of AI, IoT, and deep learning should be reinvented (Tufekci 2017) to serve humans welfare instead of the revenue of giant organizations in the Smart Society. Smart sovereignty may be accomplished by concentrating on technology, education, and government to guarantee that individuals are true sovereigns in charge of their own lives and futures (Aldabbas et al. 2020a).

Smart Sovereignty prioritizes humans, with a stronger emphasis on the environment, society, and people's best interests and prosperity. The 4IR (Schwab, 2016), which will pave the way for Smart Sovereignty to shape the future of the Smart Society, focuses on values, ethics, and privileges, particularly from a digital perspective.

To address future concerns and include policymakers, educational institutions, and other impacted parties, a new strategy is necessary. The strategy should underline the need to

develop a roadmap to achieve the intended results. This summary of Smart Sovereignty's goals and tasks crystalizes the definition of Smart Sovereignty as in Box 4-1:

Box 4-1: Smart Sovereignty Definition

> **Smart Sovereignty** is "a self-governing right entity of individuals in Smart Societies to retain their societal security"

Hence, Societal Security – as defined in this dissertation – means "protecting individuals and their values and ethics in a smart society from any risk and threat that is technology-related to meet human security needs"(see chapter 2.2.2 Societal Security).

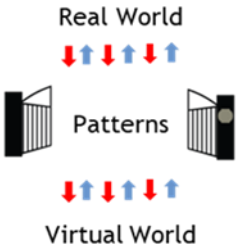
Sovereignty, in this sense, is digital, apart from the political domain. Smart Societies like Society 5.0 and 4IR are about more than just privileges; it is also about individual responsibilities to enable them to be true sovereigns. Just as citizens in conventional sovereignty had duties (i.e., paying taxes, serving in the military, electing their representatives), citizen in a digital society can only keep their rights and independence if there are active members of the digitalized world. As we currently expect citizens to report serious crimes if they witness one or help another person in danger, the digital sovereign should not allow illegal use of its data or take part in unethical or illegal actions while using digital services. The perception of online crimes might be different from conventional ones because of the distance between an individual's interaction through a screen, but as explained before, the effect on individuals is as significant as for a conventional crime. Therefore, Smart Sovereignty is necessary to avoid indulgence in the misuse of smart technologies. The fields of applying smart sovereignty are mainly: energy, mobility, healthcare, and life quality to achieve societal security. Smart Sovereignty is eligible to become an international phenomenon with its specs to meet the needs of many countries and nationalities.

Smart Societies need popular sovereignty, which is a worldwide requirement. The control of citizens over technology is low because of its complexity. It mimics a battle between people and robots to fully utilize the capabilities of all technology in the service of human values (Aldabbas et al. 2020a). Nonetheless, the control of people on their digital integrity will allow it to evolve in the desired direction and not randomly towards what each service provider wants to implement. Smart sovereignty must be enforced with additional resources than just the will of the individuals and must become a habit for developers, IT specialists, data

engineers, and civil servants that will carry on their tasks on digital platforms. Regulation authorities must continue their mandate to control existing businesses to allow them to grow in the right direction, and law enforcement agencies must also oversee citizens' protection from smart criminals.

In Smart Societies, the goal of Smart Sovereignty is to maintain individual and societal security. There is a need to promote awareness of Smart Sovereignty, which multilateral organizations rather than individuals should lead. Instead of expecting awareness to emerge naturally among people, organizations, and administrations, raising awareness must be a planned and intentional endeavor. These groups should represent the people and have legal credentials regarding support and guidance to avoid Smart Societies becoming machine-focused, which is one of the issues that Smart Societies will face. Governance methods must monitor technology (Aldabbas et al. 2020a).

Data is the cornerstone of the virtual world, as discussed, and it is at the heart of Smart Sovereignty. Actors (humans) in the physical world are linked to data in the virtual world through platforms and patterns controlled only by huge businesses, governments, and/or government entities. Individuals, and by extension society, are reliant on and at the mercy of these power pillars, which is not a desirable or healthy setting for a Smart Society. Figure 4-6 (Aldabbas et al. 2020a) shows the interplay between the actual and virtual worlds and how platforms serve as a bridge between both worlds.



People	Real World Protect data, people's privacy, assets
Patterns	Platforms and Interfaces being the gate
Data	Virtual World Strategic part Predict data Memory of real world

Figure 4-6: Interaction of Real World and Virtual World (Aldabbas et al. 2020a)

Developing, improving, using, and protecting new patterns to build a Sustainable Smart Sovereignty framework are key responsibilities for achieving Smart Sovereignty. Smart Sovereignty requires fresh data patterns, given that huge corporations currently hold most data patterns. Such designs need much money and security to imagine and develop (Aldabbas et al. 2020b).

The loop of achieving, maintaining, and improving sustainable Smart Sovereignty begins with the realization of Smart Sovereignty through its application in Smart Society, followed by making sure that people are the true sovereigns in their societies and that they have the authority to examine, govern, and alter the course of technological development for it to serve their interests as humans. As time passes and circumstances change, some shortcomings in using Smart Sovereignty may become apparent, necessitating the system's flexibility and acceptance of changes as an inherent part of the Smart Sovereignty life cycle. The fresh inputs and changes will impact nature, and likely use of Smart Sovereignty, and an amendment of Smart Sovereignty will be ready to be deployed in society (Aldabbas et al. 2020a). Finally, it is necessary to emphasize that this framework for long-term Smart Sovereignty is simply the first draft and is susceptible to change as the development of Smart Sovereignty progresses.

4.3 Features of Smart Sovereignty

Starting from the fact that data is the core component of a smart society (Aldabbas et al. 2020b), most of the focus on sovereignty will be data-oriented. However, one should not get carried away and omit the other components of a smart society and smart sovereignty. It has long been understood that countries, administrations, and their people should not receive absolute unrestricted freedom in cyberspace (Wu 1997). The internet is regulated, which is a correct step to increase security in societies globally. The benefit will affect nations, companies, corporations, and private citizens are well. However, there is a conflict as many states try to increase their power and boost espionage to limits that violate their citizens' human rights. Therefore, cyberspace designers must create logical standards and regulations that can gain wide acceptance globally and provide necessary protection for people in cyberspaces.

Several new and old studies and reports shed light on the importance and the necessity of internet sovereignty, sovereignty in cyberspaces (Min Jiang 2010; Wu 1997; Goldsmith 2017; Budnitsky and Jia 2018), and data sovereignty (Peterson et al. 2011; Kukutai and Taylor 2016) for the present time and the future. Much emphasis was put on social topics such as digital trust (Gräf et al. 2018) and digital ethics (Floridi 2018) to be integrated into processes like manufacturing and developing digital products, especially for smart devices. However, to the best of the author’s knowledge, no study has addressed sovereignty as a concept in a smart

society or dealt with sovereignty as a core element for security in a smart society despite its relevance to the people individually and as a society.

The significance and sense of digital trust for smart sovereignty

Digital sovereignty is different from Smart Sovereignty. Nevertheless, Smart Sovereignty has also a digital nature. It is important not to mix those two terms. Every user of technology, whether we speak of a human being, legal person, or governmental entity, everyone wants to have full control over their data in cyberspaces and be protected from intruders (Gräf et al. 2018). In other words, everyone wants to be digitally sovereign. That is particularly important for individual users, especially when trust levels of rules and regulations are low. Luckily, people's trust in their government's performance is not necessarily associated with their trust in aspects of the e-government service. Trust is rather affected by the financial support for e-government. Most governmental internet clients tend to trust e-government services (Horsburgh et al. 2011). In recent years, a broad social discourse on digitization's potential risks and opportunities has evolved under digital sovereignty. Various actors use this term, each with their objectives and understandings. Altogether, the state of being digitally sovereign carries different meanings for states and individuals (Gräf et al. 2018). However, the definition of digital sovereignty does not exist yet. Not only that, but also there are different contexts in which it is used, and each has a different interest and vision.

Stakeholders in Smart Sovereignty

Several stakeholders are considered components of smart sovereignty and an important success factor. This section gives an impression of which individuals and governmental bodies can compose the stakeholders for smart sovereignty. To a certain extent, the classification of stakeholders was inspired by (Gräf et al. 2018) as they defined role actors in Germany in their analysis of digital sovereignty:

1. Political actors in Switzerland (heads of parties).
2. Ministries: education and higher education, economy and development, communications. Advocates, heads of transportation, digital legislation, and policymakers.
3. Clubs, associations and, civil society, federations in the field of digitization.

4. Scientific environment. Smart sovereignty should receive interdisciplinary attention in various fields: political, economic, ethical, psychological, and so forth.

Challenges for Smart Sovereignty

The challenges to reaching smart sovereignty mostly lie in the lack of capabilities and availability of necessary conditions and requirements.

Among the many challenges, (Gräf et al. 2018) stressed some of the following hinder digital sovereignty: 1. Espionage using digital channels, both between states and in the economy, continues to pose an unmet challenge to digital sovereignty. 2. Security against digital crime from viruses, ransomware, and identity theft. Cyber security issues are yet to be structurally guaranteed. 3. Economic dependencies regarding the availability and development of key technologies represent an obstacle to self-determination. 4. The market power of foreign and non-European monopolies restricts the choices of companies and users. The root cause of this major problem is that Europe and America allowed China to be the world's factory (Mees 2016) and the world's pharmacy. 5. The competence of many Internet users still needs to be improved in both private and professional areas as there are still significant inconsistencies in information and power between online platforms and users. In addition, there is often no transparency regarding personal processing data, and the control options for users in this regard are also extremely rare. 6. There is a high level of group pressure that encourages the use of data processing despite widely known power imbalances and the lack of control over data processing.

There should not be a strong distinction between smart sovereignty on the national level and smart sovereignty for individuals and businesses. The reason is that the challenges to security and well-being arise from various sources, but they are interrelated in many different ways (Gräf et al. 2018). The concept of smart sovereignty is designed to include and consider different entities but individuals. The sovereignty of the individuals in the sense of freedom from outside interference and self-determination has legal status. One can only be a real sovereign if he lives in a sovereign country. Evidently, being a sovereign state is a pre-condition for having sovereign people. Additionally, other sectors must guarantee freedom and sovereignty for the individuals, such as a free press (Gräf et al. 2018). The message here is to assure the need to avoid discrimination between the components of sovereignty as they are strongly interdependent and interrelated.

Social context and governmental challenge

Social context is a unique social, cultural, and political mixture pattern. The societies with characteristics and attributes of respecting democracy and human rights have a gravely different social context to societies ruled by dictatorships and fascism (Mostaghimi 2006) governments like Syria and Iran. In the case of such dictatorship regimes, IT will be used to control social relationships, and monitor and spy on people, while in a democratic and liberal regime, governments often attempt to base their laws according to the consent of the people (Mostaghimi 2006). The concept of sovereignty is related and strongly connected to social context and is being confronted constantly with the strong influence of IT and globalization on society.

More insight into the value and the limits of the concept

A conscious and purposeful approach to a state of smart sovereignty depends on how comprehensively one understands this concept. That is necessary because smart sovereignty is suitable as a concept and an identification of a state for many actors. A wide range of actors, such as internet users, can unite behind the concept when they have mutual interests. However, the interpretation of smart sovereignty can lead to a conflict of interest in the form of misinterpretation and misuse of the status of being a smart sovereign.

There is some vagueness about applying the concept in practice when it comes to the limitation of smart sovereignty. The concept hits its limits in terms of its suitability for international actors simply because it is unclear which state is a smart sovereign state and which states are not.

For an illustration of this problem, let us imagine this scenario. A man from country A is married to a woman from country B. They have children together, but they all live in country C. They go on vacation to country D, where a fight happens between the couple, and the man accidentally kills his wife and escapes to country C, where the police arrest him. Now the question is: shall he be presented for trial according to which law? Of course, if they all were from country A and lived there too, and if the crime happened there, it is easier to judge and say they are subject to the law of country A. However, in this fictive example, one needs a legislator who knows international law and can eventually provide an answer. Now, despite all the international legislation for laws and crimes, conflicts and disagreements still happen

between countries over such cross-border crimes. Likewise, smart sovereignty will require regulations to organize potential future conflicts of interest.

In data sovereignty, it is still unclear who determines what happens to own personal data. There is even a debate about whether data can be owned or not (Gräf et al. 2018). For instance, the owner of a photograph, according to the United States copyright office, is the photographer or his employer, not the person being photographed (U.S. Copyrights Office 2021). In Germany, the Federal Ministry of Transport and Digital Infrastructure spoke out in favor of specifying such ownership in new data law. However, data protectionists believe that ownership of personal data is incompatible with the applicable law and the principles of data protection (Gräf et al. 2018). In Switzerland, Legislation largely governed the concept of data sovereignty to guard against data misuse. For open data, especially for open government data, there is a lack of legally binding regulations. The right to data portability is included in legislation on personal data, which nevertheless focuses primarily on data protection. It will be important to decide who owns and makes use of the data gathered in Switzerland or generated by Swiss residents. Switzerland's data sovereignty is seriously threatened by the rising exclusive concentration of data on a small number of international platforms. To ensure that all of Switzerland's citizens, political entities, businesses, administrations, and other institutions and organizations will be able to use their data in an optimized and self-determined way going forward, there are several legal, organizational, technical, and educational measures that must be taken at all levels (Golliez 2022).

Furthermore, what individual data are worth is unclear. The value depends on the context and how they are aggregated and used (Gräf et al. 2018). For example, there are debates about making personal data a payment method for apps. Consequently, the apps labeled “free” are not, as they receive users’ data in return. Moreover, it is unclear who should access which data and under what circumstances. For example, in logistics, various actors would have a legitimate ownership interest or the right to access mobility data: Vehicle users, vehicle owners, vehicle manufacturers, suppliers, infrastructure operators, and insurers (Gräf et al. 2018). Legislators and software developers will require access to this data to improve existing transportation methods and solve problems that matter to society, like in the moral machine experiment that deals with the challenge of measuring societal expectations concerning ethical principles that should lead the behavior of the machine (Awad et al. 2018).

The concept of data sovereignty suggests a capacity for self-determination over one's data, but it is often unclear to whom this data ultimately belongs. This problem remains unsolved, and no accepted norm has yet emerged (Gräf et al. 2018). At this point, this problem symbolizes a gap in the smart sovereignty concept and should be considered when developing approaches to strengthen sovereignty.

Improving sovereignty and overcoming challenges

There are several opportunities to improve smart sovereignty. The efforts to strengthen smart sovereignty involve collaborations between the stakeholders to develop a coherent strategy to develop sovereignty (Gräf et al. 2018). Therefore, it is important to precisely define the underlying understanding of smart sovereignty and its objectives (Aldabbas et al. 2020a) and to take a close look at the context in which the respective efforts are to be made (Gräf et al. 2018).

Technology, competence and knowledge, social structure, and regulations are the main approaches to counter the challenges to smart sovereignty as (Gräf et al. 2018) argue. These approaches can focus on individuals, companies, and the entire system. In many cases, synergies can arise between individual factors. For example, improving basic IT knowledge and core digital competencies for individuals will benefit companies and countries equally. That will allow users, employees, and clients to help the organization achieve a suitable structure and help the organization reach a smart sovereign status.

Technology and sovereignty

The development and design of technology are crucial for smart sovereignty. Information technology and the freedom of technologies, which implies the notion of technology sovereignty, increase people's competencies to create data and connect (Mostaghimi 2006). Accordingly, there are diverse approaches to using technology to strengthen smart Sovereignty with the help of technology. These measures will require European collaboration to develop, produce, and refine key digital technologies, services, and platforms. That means gathering collective efforts through smart collaboration, coordination, and funding. It also involves building and sustaining capabilities to test and evaluate digital technologies, services, and platforms from a performance and security perspective (Gräf et al. 2018). The latter cannot be done without ongoing education and acknowledging the role of educational sovereignty in the

quest for smart sovereignty (Moll 2002). Cultural, social, and technological aspects must be considered all the time, as the components of smart sovereignty are interrelated and interactive.

Technological reform needs the implementation of modern and suitable data protection principles that protect the concept of “Privacy by Design" and "Privacy by Default" to motivate the development of new products (Gräf et al. 2018). Intellectual property protection has become more crucial than ever with the digital wave. Since approximately 2005, this issue began to be systematically regarded as a national security threat to the United States. The extent of intellectual property theft involves hackers, trade secret theft, and illegal data sharing, and at the same time, the external students registering in American universities were seen as part of this threat (Halbert 2016). Therefore, European legislators need to embrace a strong intellectual property rights system, which will help strengthen smart sovereignty. China has long been working on a new intellectual property rights regime which was becoming trendy and gaining momentum in China, but this new regime has not been paid enough attention in academic literature. Studies and analysis show that China embraces a strong intellectual property rights system. Meanwhile, the United States is heading toward a weaker system (Nguyen 2011). Europe needs to be up to the challenge and redesign intellectual property rights as the significance of this issue only increases with time, especially with the world turning digital.

Moreover, the development of digital applications whose main purpose is enhancing the smart sovereignty of their users should include personal data stores. That allows users to manage and control the distribution of their data when dealing with managing and controlling their data (Gräf et al. 2018). Further measures to support sovereignty via technology show the need for special consideration of the security of products and offerings. The IoT is the new leading technology in terms of digitalization and smart computing. However, one huge downside of IoT systems is the absence of confidentiality and security that safeguard schemes for monitoring and restriction access, and guaranteeing data safety (Sreelakshmi et al. 2021). Particularly in the emergence of IoT and IIoT regularly causing difficulties and sometimes damage due to security deficits. There is a need for increased improvement (Gräf et al. 2018). Blockchain technologies offer novel approaches to closing security gaps in IoT. The security of IoT is being challenged by attacks and random damaging games, but the blockchain has the

potential to be the main empowering force to handle immense IoT weaknesses (Jain et al. 2021). Many studies and experiments have been in the arena of merging IoT and Blockchain. Results show promising progress in addressing certain important matters in IoT security problems (Sreelakshmi et al. 2021)

Competencies and knowledge

The smart sovereignty of an organization depends a lot on the sovereignty of its personnel. Therefore, a person's smart sovereignty will rely significantly on digital competencies. There are indeed constructive approaches that can support the digital competencies of individuals. Following the suggestions of (Gräf et al. 2018), the subsequent paragraphs illustrate a few approaches that should assist in broadening the horizon of smart sovereignty, in addition to other arguments and statements that need to be considered.

The discussion about the digital competence of cyberspace users is complex and contains various valuable proposals, such as teaching the principles of computer science in elementary school education (Gräf et al. 2018). (Aldabbas et al. 2020a) discussed the importance of involving education to strengthen digital competencies. More recently, under the challenging circumstance and the difficulties that the Covid-19 pandemic poses to the world and especially to education, serious issues discussed in (Aldabbas et al. 2020a) arose faster than anticipated, such as cyberbullying and technology addiction.

The pandemic has triggered rushed digitalization for primary and secondary schools around the globe. Cyber threats such as harassment, cyber addiction, deception, and propaganda need to be tackled immediately. Studies such as (Jackman et al. 2021) urge the necessity to synchronize international endeavors for basic digital skills education. Otherwise, students might not survive the digital waves without disturbing serious damage in cyberspace. It will be the task of teachers in schools and the educational system in general to increase further education for teachers in digital skills (Gräf et al. 2018). The states have extensive scope to act and should be held responsible and accountable in case of failure. The German Council of Consumer Advisors also recommends providing more financial support than in the past for extracurricular programs to promote digital literacy (Gräf et al. 2018). Moreover, beyond digital literacy as competence primarily in the use and handling of digital and cyberspaces, there is also the approach of strengthening the ability to be critical of technology as a

competence. That relates to the shaping of technology and is particularly relevant for the independent attribute of smart sovereignty (Gräf et al. 2018).

To conclude, the extensive digitalization of the educational sector is already occurring. Fortunately, the Coalition for Digital Intelligence, in partnership with the WEF, endorsed the IEEE Standard for Digital Intelligence Framework for Digital Literacy, Skills, and Readiness. These internationally recognized standards can create a shared framework to coordinate digital skill-building endeavors worldwide(Jackman et al. 2021). However, it is the responsibility of all interested parties such as government, society, civil society, and international organizations to guarantee digital transformation. At the same time, students are equipped with strong knowledge and digital tools to reduce the drawbacks and threats accompanying the rising wave of digitalization in education.

Often, there is a problem that people are unaware of or do not attempt to do anything about it. It is about the wasted competence and the forgotten skills which are not being used by those who have them. Even people with advanced developed competencies come up against limits if there are no opportunities to use them or if they are only used to become aware of their limited smart sovereignty (Gräf et al. 2018). Therefore, to avoid and limit the effect of wasted opportunity, the design of the digital ecosystem at the societal level is an important area that can offer powerful approaches to strengthening the use of the skills for enhancing smart sovereignty. Strengthening the control and protection structures in terms of staffing and funding, such as consumer centers and data protection authorities, can indirectly strengthen the smart sovereignty of the population (Gräf et al. 2018). Conventions, such as using open-source software in private and public structures, can help establish trustworthy systems and strengthen smart sovereignty by increasing the digital skillsets of users and stakeholders (Hofferbert 2020). However, one must be aware that thinking in black and white when dealing with open or closed-source software is not the best idea. Since open source is neither generally safer nor is proprietary software vague across the board. As is often the case, the truth lies somewhere in the middle (Hofferbert 2020), and one needs critical thinking when selecting an approach.

Regulation and laws

Digital regulation and intellectual property laws need to change to cope with the digital age in the smart society. Regulations should further improve to strengthen the smart sovereignty of

people and other entities for the future society. In this context, the following paragraphs present challenges for regulation that are particularly relevant to smart sovereignty in three major focuses (Gräf et al. 2018) and the focus on digital sovereignty. Additionally, the challenges for regulation and supervision that touches financial innovation in the digital age (González Páramo 2017), and certainly not least the digital Governance and soft ethics (Floridi 2018).

The approaches to change for digital regulation should be oriented to improve the transparency of data processing operations and strengthen the smart sovereignty of all those affected. That requires regulatory steps, especially in automated and data-based decision-making processes (Gräf et al. 2018). To counteract the formation and consolidation of monopolies, binding standards for the interoperability of certain digital services could be useful.

Data Structures and Algorithms are at the core of computer science. Certification of data structure and algorithms by experts from around the world can carry benefits for users and industries. This also supports the users and provides consultation that adds to their knowledge of the matter on hand. It offers software programmers a licensed standard and provides access to certified software engineers globally and not limited to the local market within the state, in addition to contributing to computer science students' education by providing genuine training opportunities (Kalbalia 2021). The idea of a quality certificate for an algorithm could ensure, under certain circumstances, that this algorithm copes with the existing standards, for example, combating discrimination and not revealing trade secrets of digital companies to third parties (Müller 2021).

Banks and financial institutions could always crack out the best of technology in their favor, enhance their effectiveness and productivity, and consequently improve their clients' products and services. However, banks these days are faced with a new wave of creativity and digitalization that come with broader repercussions for financial services (González Páramo 2017). Despite the non-questionable advantages of technology, the advances and their consequences on the effectiveness, economic stability, client protection, and transparency of the financial system need a comprehensive overhaul by legislators and monitors (González Páramo 2017).

A deep analysis is necessary to accommodate the changes in digital security to guarantee the security of customers and clients and, simultaneously, prevent banks and financial institutions from abusing the data they have. The issue is that the new digital paradigm introduces new threats to cyber security, safeguarding clients' data and information and protecting assets from outsiders and insiders.

Preparing for future crises will require investigation as they will come with an unprecedented nature. The newly required overviewed legislative and regulatory structure has to completely encapsulate the advantages of digital innovation in the banking and financial sectors. The newly built system must be robust when facing future financial crises (González Páramo 2017).

The enhancements and reformulation of existing legislation should focus on several key areas (González Páramo 2017): 1. Review policies that oversee the control and administration of the emerging risks triggered by technology in the financial sector. 2. Initiating innovation centers to continuously support and supervise the technological transformation. 3. Promoting safe environments for market research before implementing technological changes in the industry and analyzing the drawbacks during the testing phase. 4. Focusing on expanding digital skills and promoting a collaborative mentality.

Smart Societies' fundamentals are built on data, and the connection between the real and virtual worlds goes through the platforms. So the platforms are the gate that teleports us between worlds (Aldabbas et al. 2020a). Without data, a Smart Society would not exist, and interaction with the virtual world would not materialize similarly without an interface. Considering Smart Sovereignty, accessing digital services is strategic for users, lawmakers, strategic firms, and technology providers. For further understanding of these platforms and their role, it is recommended to visit (Aldabbas et al. 2020a). The word sovereignty in cyber security was used before as several research papers addressed its significance (Wu 1997). The concept of Smart sovereignty goes beyond that scope and considers further requirements for the citizen to remain sovereign in a smart society.

In democratic and liberal nations, one of the internet's roles is to promote liberty and freedom of speech and eliminate racism. Unfortunately, the reality proves this does not happen as much as necessary (Aldabbas et al. 2020a). Access to digital content, if it remains unsupervised content-wise, can guarantee access to plural information and knowledge and create a link between individuals. It supports free speech and allows people that would not have had access

to a public audience to make their voices heard. However, this idea that the internet should be a neutral medium is currently challenged on many levels.

Many authoritarian countries like Russia and China exercise questionable practices as they exploit the internet and use it to police, monitor, and spy on all citizens. Additionally, the internet became a tool to emphasize their authority (Jiang 2010). Such control through internet service providers or ISPs reoriented web access from being an empowering tool for the citizens to a medium of opinion shaping used by well-established political powers. Currently, the idea of the free and open internet is being outweighed by the commercial and political use of research algorithms and social network bubbles to shape citizens' desires and opinions.

Furthermore, with the growing use of the internet for daily activities, issues have arisen, creating a whole field of research. Smart societies require defining digital ethics to handle with care the impacts of digital transformation and the increasingly sophisticated communication means in society. These matters are not limited to social division, governmental surveillance, cyber-bullying, cyber-addiction, and manipulation (Capurro 2009). Those complex issues show how the evolution of society together with digital services and information can produce both positive and negative outcomes. Smart societies are challenging the technical necessity, the complex innovations, and the governance and surveillance of all digital features in every possible domain (Floridi 2018). To develop a performing society digital society, the challenges mentioned above need to be addressed. In the event of imbalances, rising social issues will decrease trust in smart technologies. Understandably, negative outcomes such as invasive surveillance from the State or opaque exploitation of data for commercial purposes without transparency could lead citizens to avoid technologies and devices that made it possible. Reaching effective efficiency and exploiting IoT and the accompanying services cannot be reached in a society if the factor “trust” is not properly addressed (AlHogail 2018). In addition, social acceptance and any new technology's active appliance are deadlocks unless the user’s trust is open. Smart sovereignty is based on automation and digitalization to reach a modern reformation of the comprehension of the real role of digitalizing, and that will need a harmonization in the process of interconnection between humans and smart technologies and devices, which is certainly not a bubble, but rather turning into a lifestyle (Teufel and Teufel 2019). Without trust, one can easily forget about fruitful digitalization and peaceful social transition. With this evolution, an individual’s integrity will be challenged if it is not protected

correctly. Smart Sovereignty will allow them to keep control over their digital selves as traditional sovereignty protects citizens from external influence in existing societies. If implemented correctly, smart sovereignty will then empower individuals in smart sovereignty to keep their rights and their integrity intact in a fully digitalized world. Digitalization has become a tool, particularly in a smart society where individuals have a key role in making a smart society work (Shiroishi et al. 2018). The importance and the power of digitalization are weighed by the changes they will bring to society in the form of technical innovations, process optimization, lifestyle improvement, and social progress (Teufel and Teufel 2019). Every process of industrial society can be improved through digitalization to optimize production and services. If such goals are fulfilled, citizens of a smart society could access better living standards sustained over time by efficient use of resources and automatized processes. However, this ideal digitalized society is not a given, and the rearrangement of the method of digital technologies and innovations function is gaining more importance and significance these days (Tufekci 2017).

Elements such as IT improvement procedures, economic incentives, increased AI application and ML transparency, and data gathering needs to be carefully studied and integrated into a sovereign society (Aldabbas et al. 2020a). Only by controlling technology development and usage will society be able to promote the benefits of digitalization over side effects. That requires conscious actions and technological development, regulation, and practice monitoring. There is a need to define human goals and priorities of technology development first, then integrate these into the building processes of AI (Tufekci 2017). The strong potential of AI can provide meaningful upgrades to current services, but its complexity makes it even harder to monitor. Russell (Russell 2019) argues that AI needs a redefinition to guarantee that the benefits of the built machines are in favor of society.

The environment of smart sovereignty will hinge on knowing the nation's political-ecological and technological current state (Aldabbas et al. 2020a). Expected benefits are tied to social and economic contexts and will allow better use of existing digital services. Depending on the type of services, challenges answered through smart sovereignty will not be the same, and potential outcomes are expected to vary accordingly. Consequently, this means that the features of sovereignty will most likely not be the same in each country where it applies. However, general

global standards could still be established. Afterward, it becomes possible to adjust according to the particularity of the hosting environment.

4.4 Domains and Applications of Smart Sovereignty

The application of smart sovereignty can be quite broad. Within this framework, two main aspects of Smart Sovereignty are particularly important: data protection and digitalization. These two aspects form an umbrella covering all the application fields of smart sovereignty as presented in Figure 4-7 based on (Aldabbas et al. 2020a).

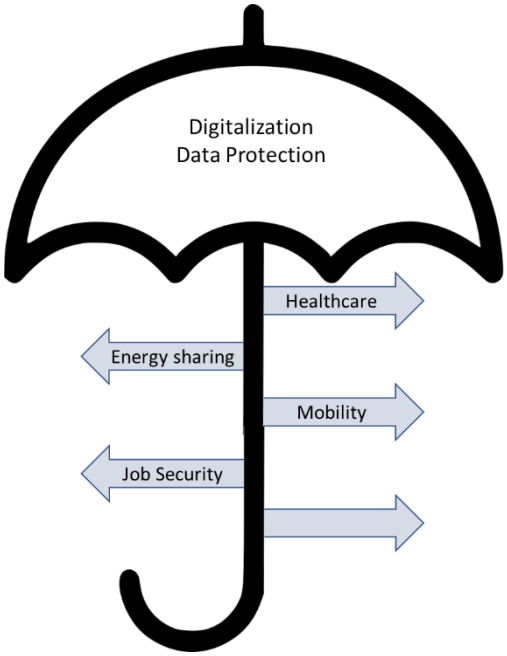


Figure 4-7: Application of Smart Sovereignty, based on (Aldabbas et al. 2020a)

The well-being of humans depends on many factors (OECD 2022) as illustrated in Figure 4-8. The focus is on healthcare, mobility, energy sharing, human well-being, and other fields directly touching our lives. These were properly addressed in chapter 2.3.

Healthcare relies mostly on human-to-human interactions and should continue to do so. Social and emotional support are part of it. Several aspects of healthcare can be improved and accelerated with smart technologies. Healthcare facilities and workers are progressively trusting machines, mainly in surgeries.

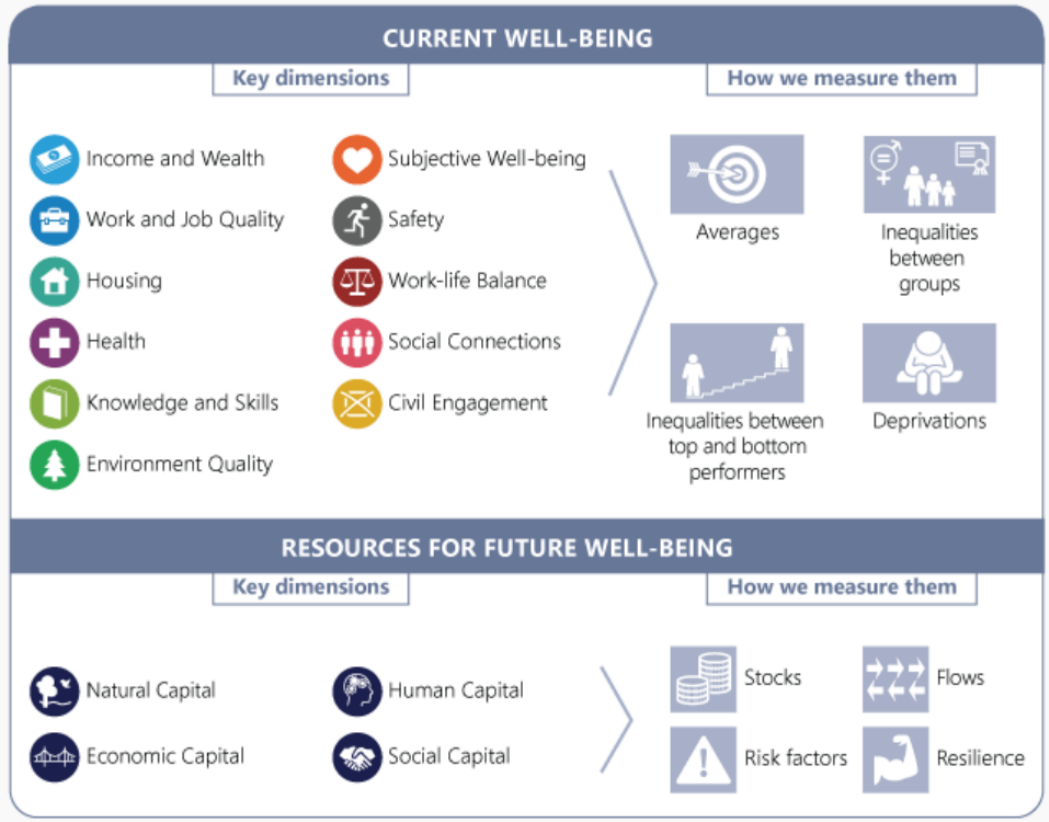


Figure 4-8: Human Well-Being (OECD 2022)

Medical files, history, and information also tend to go toward more digitalization to ease the exchange of information between practitioners. That also extends to smart diagnostics that can improve doctors' decision-making and make diagnostics faster and more reliable. Overall, those new fields allow for the collection of data that will inform scientific studies and improve the training of future healthcare professionals. However, despite all possible benefits, healthcare in a smart society is also confronted with new threats.

According to one research (Lindner 2017), there are considerable gaps in defenses against fundamental kinds of cyber-attacks. Both the protection of patients' private data and the settings of the software that drives the robot during an operation have been recognized as having security flaws. Third parties can simply modify the point's coordinates of inserting the knife during surgery, for example, to launch a malicious assault. The current scenario shows many flaws that must be addressed immediately and comprehensively to prepare for Society 5.0 (Aldabbas et al. 2020a).

The use of/reliance on sensors, information, and communication technology will be one of the primary features of the Smart Society. The existing technology will enable creative energy-

sharing concepts like Crowd Energy (Teufel and Teufel 2015) and smart grid-based energy generation and transformation. That implies that any security flaw in the grids might jeopardize the integrity of the energy exchange. Previous research (Teufel and Teufel 2019) found that crowd applications may be designed in the energy sector, so crowds become Smart Society enablers, achieving one of the primary aims of Smart Sovereignty. Because most of the need for mobility is based on sensors and information and communication technology (SICT), mobility in Smart Societies is crucial and challenging (Aldabbas et al. 2020b; Ducrot 2019).

Now back to the main domains, data protection, and digitalization. Those areas of interest will have the most impact on society. Many works sufficiently addressed data protection (Chen and Zhao 2012; Aldabbas et al. 2020a; Bloomberg 2015). Smart societies will use data as a cornerstone and be completely data-dependent. Without big data and proper data care, which is the backbone of the smartness of society, there will not be a smart society. Data goes through several phases, from when it is generated to when it is destroyed.

For some researchers, there are seven phases (Bloomberg 2015): capture, maintenance, synthesis, usage, publication, archival, and purging. For simplification, it is possible to say that data has five phases (Aldabbas et al. 2020b): collection, communication, storage, usage, and destruction. Note that all seven phases from (Bloomberg 2015) are integrated into these given phases. Those steps should exist for every field the Smart Society develops and will apply as a complementary layer to considerations specific to each field. Omitting the significance of data for Smart Sovereignty would be a mistake and it is not possible to insist enough on how despite other focuses and considerations. The relevance of digitalization is also addressed in more detail in other chapters and is not included in those three areas. Like data, digitalization should be addressed separately as it is not a societal function that will be transformed during the shift to a smart society but rather a part of this transformative process.

Smart Sovereignty integration

The integration of Smart Sovereignty in the Smart framework starts from the Smart Framework of (Vasauskaite et al. 2017) and their definition of Smart as meeting challenges for sustainable welfare. The framework offers a suitable method for integrating Smart Sovereignty within. Figure 4-9 (Aldabbas et al. 2020a) is the application of the Smart framework on Smart Sovereignty.

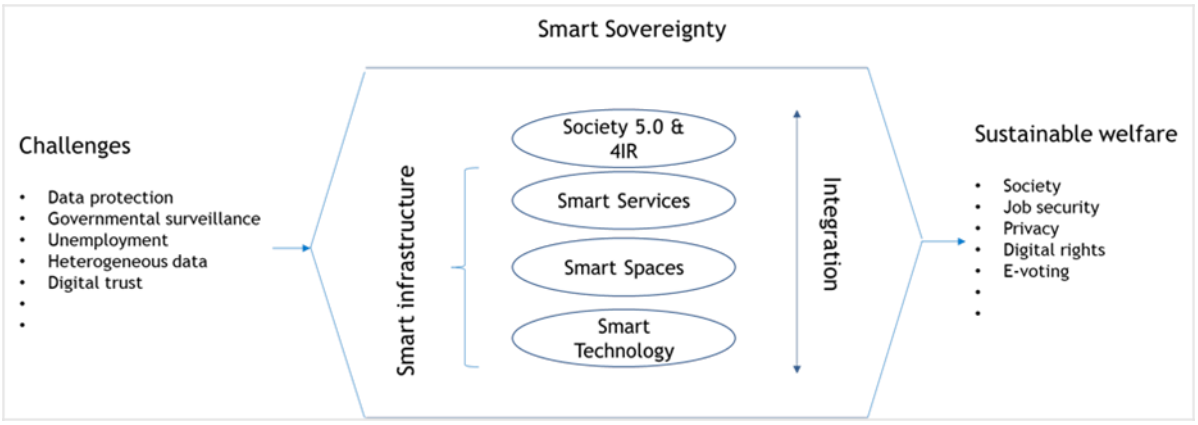


Figure 4-9: Smart Sovereignty Framework (Aldabbas et al. 2020a)

Smart Sovereignty intends to achieve long-term well-being by coordinating all activities across all layers of Smart Society 5.0. The goal is to guarantee that society, services, the environment, and technology are all sovereign. Integrating all the elements will reduce dangers and hazards, and enhance the outcomes of future development processes toward increasing Smart Sovereignty. Communities, organizations, and institutions will all need to use Smart Sovereignty one way or the other (Aldabbas et al. 2020a).

4.5 Governance for Ethics and Sovereignty

Establishing Smart Sovereignty's ethics and applying the right governing principles will create a suitable environment for Smart Sovereignty to be a success. Smart sovereignty needs to contain some sort of social system analysis to analyze the impacts of AI systems on the social level. This social system has to be publicly and broadly accepted, and it should engage in all the potential effects of AI applications on all the affected parties and stakeholders throughout all the programming stages from the basic concept, design, and then the deployment (Crawford and Calo 2016) of the end product. The system should also control the compliance of the AI systems with the laws and regulations and create alarming signals in case of violations. Many challenges currently limit the consistency of smart sovereignty governance. First, as of 2021, there is no consensus between social and political actors on the need for global data governance. Firms are currently allowed to operate as they want within outdated legal boundaries. The internationalization of main digital actors and a low level of transparency make the concept of global governance of digitalization a sweet dream but a necessary step in the evolution of our society.

In the beginning, it is important to point out different normative approaches that complete each other with harmony and should not be mixed. These three concepts are digital governance, digital ethics, and digital regulations (Floridi 2018).

Digital governance means setting up and executing rules, processes, and standards for cyberspace's appropriate development and utilization. It is a question of convention and proper coordination. Occasionally, it has no characteristic of being moral or not or legal or not. Digital governance does not include ethics in its definition and is only concerned with governance and compliance with laws (Floridi 2016b).

Digital ethics is the field of ethics that investigates and assesses moral challenges concerning data (including information), algorithms (including AI, IoT, and ML), and related applications and infrastructures. Digital ethics aims to create and enhance good morals and highly regarded values in society's technological solutions. Digital ethics plays a significant role in shaping digital regulation and governance through socially accepted morals and favored values (Floridi 2018).

Digital regulation reveals what is legal and illegal (Floridi 2018) in the digital sphere. Complying with digital regulation is necessary but certainly not enough if we wish for society to prosper and avoid ethical problems driven by technology. Figure 4-10, adapted from (Floridi 2018), shows the interconnection between digital ethics, digital governance, and digital regulations.

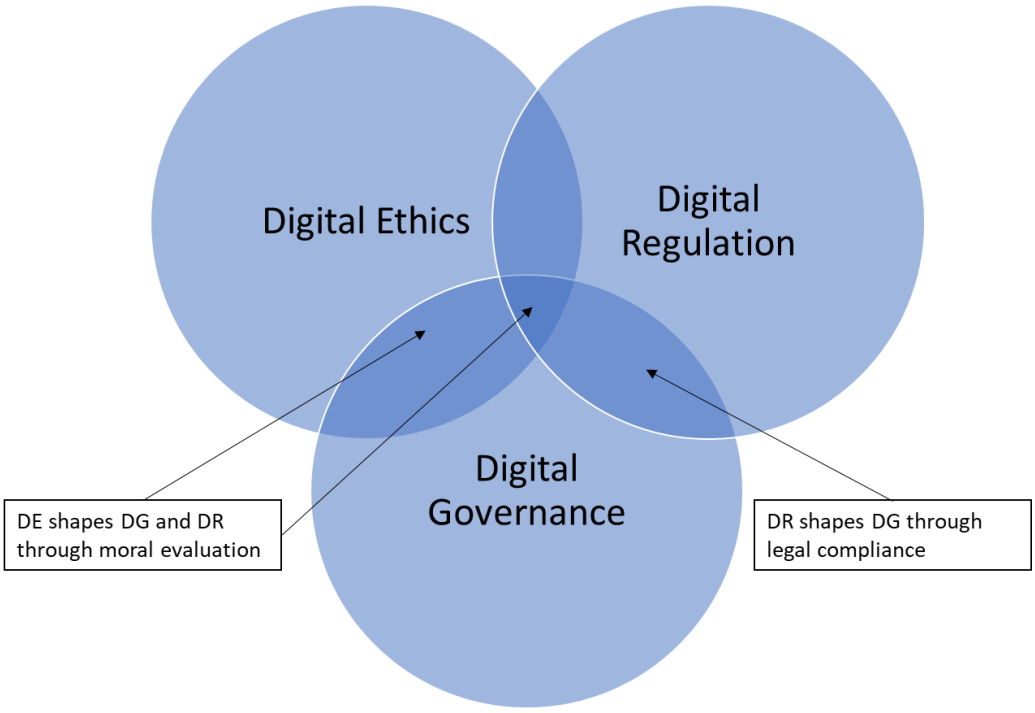


Figure 4-10: Interaction of Digital Ethics, Governance, and Regulations (Floridi 2018)

Proper governing that puts digital ethics as a priority is conditional for smart sovereignty to accomplish its goals. Reaching the goals go through four steps:

1. Including digital ethics in the design of governance, differentiating clearly between what is accepted and what is not, and not leaving gray areas where manipulations and loopholes appear.
2. Establishing and implementing rules and regulations that set the framework for effective governance.
3. Formalizing ethical standards to offer developers guidelines to decrease the probability of ethical violations resulting from technology services and applications (Winfield and Jirotka 2018).
4. Assuring and controlling that the governing body of the smart sovereignty is verifying the compliance of the software developers and the AI engineers with the ethical regulations. Figure 4-11 explains these steps.

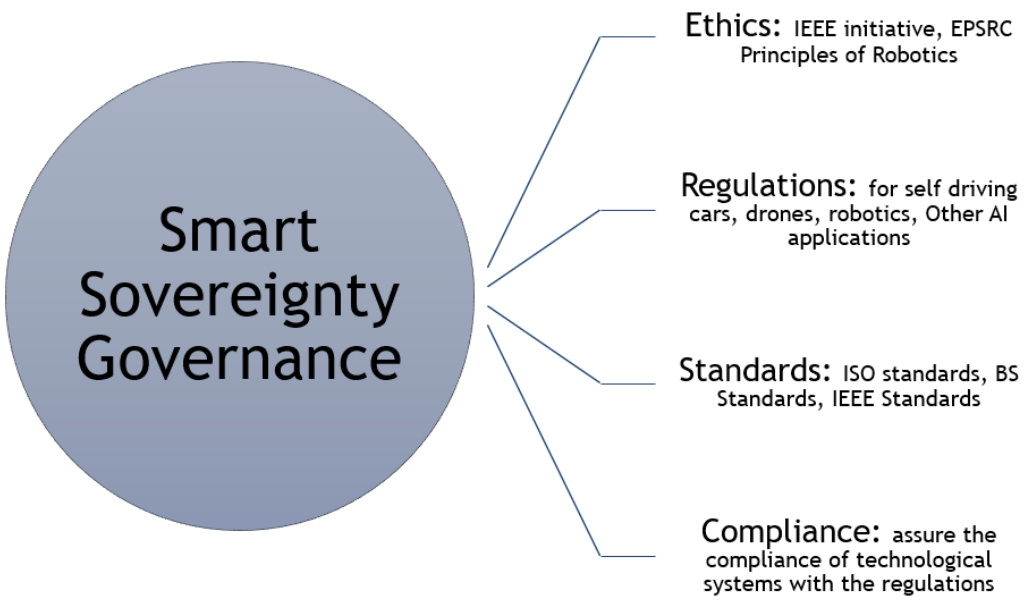


Figure 4-11: Smart Sovereignty Governance

An effective governance system implies distributing a code of ethical conduct to ensure that every individual knows his responsibility and role, especially IT employees. Promoting ethics and responsible (digital) innovation will support effective governance as it contributes to the system from its roots. Digital innovations should give human capital more priority than ever, and the emphasis should change to the complementary relationship between modern technologies and human skills. More precisely, most efforts should be fervent to a few factors:

1. Acknowledging what sets of modern IT skills will be necessary for humans in the future society and how current jobs will be affected.
2. Progression in the education system and further professional training programs.
3. Reorganizing the labor market and organizations to sustain a future where many workers will have to switch jobs and change their employers frequently.
4. Reforming social allowances systems and strengthening social safety networks to facilitate the economic transition and reduce the influence on the harshest involved workforce.

AI applications must enjoy a high level of transparency in their design. Organizations should organize ethics training for their developers and analyze and assess the ethical risk (Winfield and Jirotka 2018) to improve the quality of society and enhance effective governance of smart sovereignty. Ethical governance should be perceived as a value by society and by organizations, and it should be the responsibility and accountability of everyone. Although ethical governance does not provide a comprehensive solution to technology disruption, it is still crucial to constructing public confidence in robotics and AI applications (Winfield and Jirotka 2018). It will help preserve smart sovereignty for the benefit of society and individuals.

4.6 Conclusion

This chapter discussed the necessary details about introducing Smart Sovereignty for a smart society. The focus is on the social perspective and does not extend to the technology in use. The role that data security plays is enormous as it is the backbone of the smart society. There is a need to act immediately to reduce the potential harm for the sake of humans.

This chapter presented the story of sovereignty and discussed its meaning and how it developed throughout history. The transition to a new society requires a redefinition of Sovereignty so it copes with the modern era. Sovereignty in the past had a strong political nature and is shifting now toward socio-technological nature.

Introducing Smart Sovereignty is the core aim of this chapter, in addition to discussing the domains of its applications, governance, and maintenance. People through legal organizations will become the real sovereigns once Smart Sovereignty is properly applied. This chapter presented also a framework to develop Smart Sovereignty further so it becomes more

sustainable, which will benefit everyone in society. The governance and ethics of Smart Sovereignty are important factors for its success. Switzerland will require a thorough data policy in the future to protect its data sovereignty. To implement such a program and jointly build a reliable Swiss data space, society, the economy, and the scientific community must all participate.

Chapter 2 provided the solid ground for the definition by exploring security concerns for past societies, defining Societal Security, introducing Society 5.0, and explaining its advantages. Later, chapter 3 urged the need to act to reduce the damage that will accompany Society 5.0 by conducting a thorough multi-phase analysis; theoretical, qualitative, and quantitative of risks and outlook of Society 5.0 so they are taken into consideration in the development of chapter 4 and defining Smart Sovereignty. All pieces of the dissertation are put together and make use of each other to answer all research questions.

This chapter gave a detailed answer to research question number 3 through complete research on sovereignty, what it meant and how it evolved to acquire its digital nature for the sake of Society 5.0.

What is the sustainable solution which reduces or negates the negative effects that accompany technology?

The answer is in Box 4-2:

Box 4-2: Answer to Research Question 3

Smart Sovereignty is the security solution that can protect or reduce the damage to Society 5.0 from technology-driven threats. This novel concept of Smart Sovereignty aims to put the power back in the hand of the people and make them real sovereigns in Society 5.0. Smart Sovereignty can be achieved through legal organizations, educational institutes, and collaboration between involved sectors. People will have not only rights but also responsibilities. Smart Sovereignty has a framework for its preservation and advancement. Smart Sovereignty must be sustainable with proper governance so it provides security for the society and the people.

This chapter defined Smart Sovereignty and answered the third research question. The next chapter concludes the research and discusses further the findings.

5 Research Conclusions

This is the concluding chapter of this dissertation. This chapter reviews the research results and the findings presented in chapters 2 and 3. It establishes the closing step according to the outline of the dissertation in Figure 1-2. This chapter presents those findings and shows that they form the need for Smart Sovereignty -the most important contribution of this dissertation- (chapter 4) as a solution to security in Society 5.0. An additional discussion of the findings will follow.

The next step is to conclude the answers to the research questions in Box 1-1 with further discussion, and then to derive recommendations based on the findings. The chapter finishes by pointing out the limitations of this dissertation and discussing some of the future research topics.

Figure 5-1 shows the outlook of the chapter.

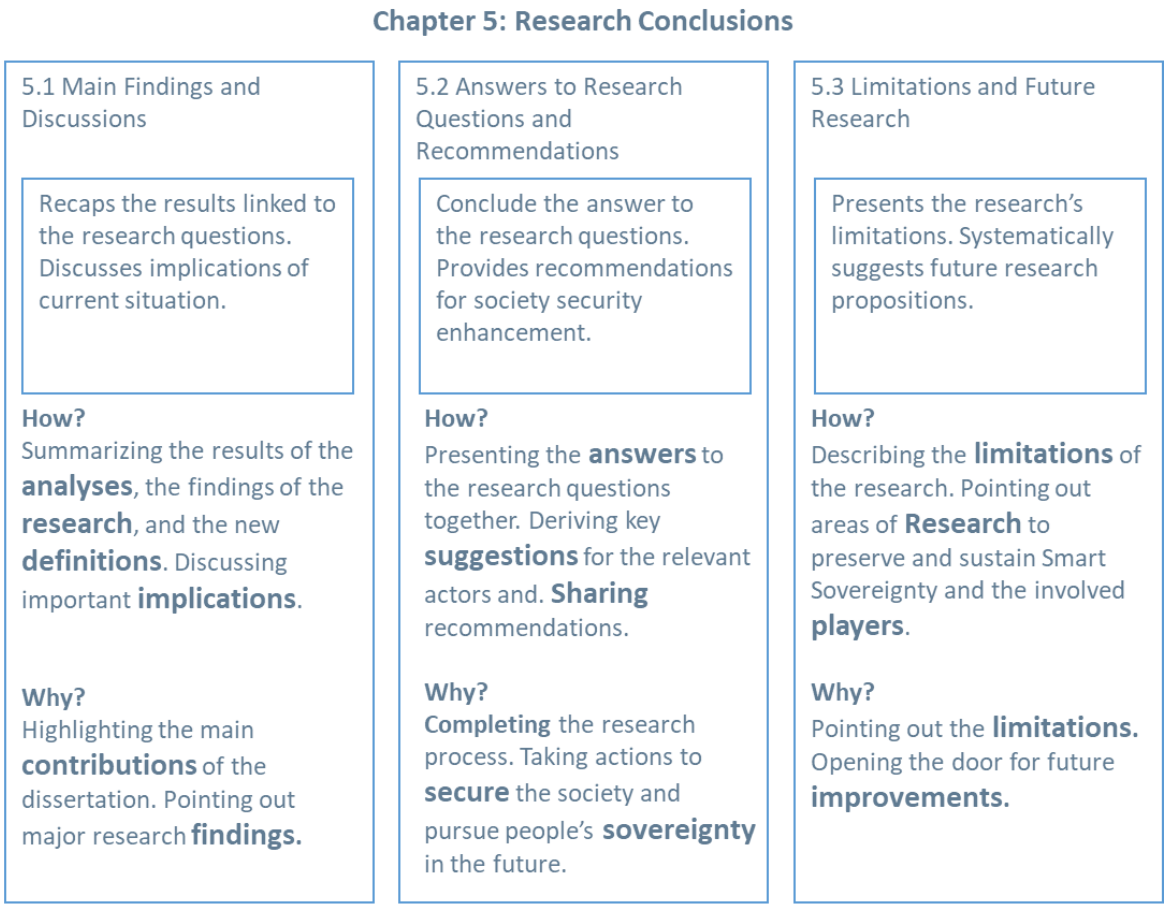


Figure 5-1: Chapter 5, Outlook

5.1 Main Findings and Discussions

The concept of security has many forms depending on the context in which it is being used. There is no consensus on the definition of security among researchers. Safety and security do not carry the same meaning in English, but they do in other languages like German. However, there are differences in their interpretation, but there is also a level of ambiguity and confusion to distinguish between them. In General, the most important elements for security are accessibility, availability, and maintainability.

Throughout the history of humankind, the notion of security evolved continuously with the evolvement of human society. The more complex the society gets, the more complex gets security requirements. The meaning of security for the first hunter-gatherer society was about safe living spaces, basic metabolic and material requirements, food, and water. For the agrarian society, security requirements expanded to cover injury on farms, population size, economic struggle, transportation costs, safe housing, and injustice. For the industrial society, security included job security, migration, data protection, international conflicts, and copyright protection. The recent information society brought new security concepts like Cyber security, data protection, and information security. The future Society 5.0 brings more challenges for security and adds many elements that require security. These new challenges are not limited to digitalization, social media, social exclusion, spying, ethics, job security, securing advanced technology, and sustaining the environment. Of course, the future society has many opportunities and advantages. Chapter 2.3 discussed the opportunities, the benefits, and the potential they bring to improve the quality of our lives.

To the best of the author's knowledge, the existing literature does not include a suitable modern definition of "Societal Security" which is very important for Smart Sovereignty. Therefore, chapter 2.2 was necessary to explore the literature for a new definition of "Societal Security" in a suitable context and then define it as:

> "protecting individuals and their values and ethics in a smart society from any risk and threat that is technology-related to meet human security needs"

Defining societal security is one of the important contributions of this dissertation.

This dissertation analyzed the risks and challenges of Society 5.0. This task was performed using three approaches. The first approach was the theoretical research in chapter 3.1.

The second approach was conducting interviews with experts in various fields and taking their judgment on matters of their expertise. The second approach was to make a forecast for some selected figures to predict how some aspects of society in Switzerland will change in the next decade. The forecast was necessary to see how technology will tangibly affect our life which cannot be found in theory or interviews.

The outcomes of the interviews suggest that the covid-19 pandemic pushed digitalization forward in society. This means that society is already changing. The pandemic offered so many lessons that society must learn from. There is a need to steer technology, boost education and adjust the education system. Swiss policymakers should be more flexible and integrate a top-down approach into the legislation. Workers should strengthen their abilities to not fall out of the new system. The state should seriously consider introducing an unconditional basic income.

The third approach is a quantitative analysis using statistics and forecast methods. The forecast suggests that the quality of life, in general, will not improve. The living and healthcare costs will increase. Future jobs will be more demanding. However, there will not be massive unemployment for the next ten years. Some sectors like retail will suffer because of digitalization. The wage disparities between socioeconomic classes will widen. Salary levels will rise in the future, but not for everyone. Employees in the ICT industry, for example, will be paid significantly more than those in other industries such as healthcare and services. Lower-income employees will face more competition for employment as more individuals are compelled to shift to lower-paying industries.

Numerous social characteristics cannot be predicted by the forecast, yet people have always demonstrated a remarkable capacity to adapt and find their way. However, this adaptation is not necessarily positive for society's ethics. As most of those people will be labeled as “left behind” or “dropped out”.

Security is like a snowball that started rolling together with the dawn of humankind. Securing the future is an ethical obligation for us humans. We owe it to the future generations that they find themselves in a world that is worth living in. The theory research on security, the

interviews analysis, and the forecast showed the need for sustainable security solutions for Society 5.0 to prevent security matters from slipping out of hand. This solution is “Smart Sovereignty”, and is the main contribution of this dissertation.

Sovereignty is an old concept of political science which had its share of evolution throughout history. This concept revolved around “the right of non-intervention”. Of course, the concept carried different meanings and interpretations depending on the historic era. This dissertation proposes a definition of Smart Sovereignty from a digital-human-social perspective for the sake of people who will live in Society 5.0. Smart Sovereignty is:

> “a self-governing right entity of individuals in Smart Societies to retain their societal security”

People through new legal entities should become real sovereigns in their societies. Power must be taken away from the high-tech giants who reign the digital world. Smart Sovereignty will need proper guidance, and proper governance to prosper and become sustainable. Smart Sovereignty is not only about rights, but also about duties and responsibilities.

Further discussion on the necessity of Smart Sovereignty for the Swiss society

The following parts discuss further important matters for the future which emphasize the urgent need to apply Smart Sovereignty in Switzerland. Switzerland needs a response policy for electricity shortages, internet cuts, refugee waves, and IT pandemics. The country has a policy for all these matters but these are certainly out of date. Switzerland needs to be proactive rather than responsive. Covid-19 showed that Switzerland has no proactive measures for pandemics. Switzerland must be prepared better for IT catastrophes and not wait for China or Russia to overwhelm the world with a new sort of pandemic. The Swiss political system follows a bottom-up approach which in some cases such as dealing with unexpected pandemics is a recipe for disaster. The variance in policies between different cantons made people very confused. Waiting for people to vote to decide on what to do in case of disaster is a disaster itself.

Covid-19, technology, unemployment

The Covid-19 epidemic has speeded up the economy's digitization and the growth of numerous supply chains. Attracting the same kind of abilities is today a competitive market across all economic sectors. One has several possibilities while looking for a career, whether he is a

computer technician or a truck driver. Numerous services have virtually overnight come to rely on digital technology because of the Covid-19 epidemic. Due to this, there has been a growth in the usage of AI applications in daily life as well as the use of mobile robots to clean public facilities like hospitals and schools. That will only increase unemployment, but the case does not look as bad as it sounds at least in the short run. In a matter of fact, the number of open positions in Switzerland in the first quarter of 2022 exceeded 100,000, setting a record. The country's prosperity is in jeopardy because of the shortfall, which might get worse. According to the most recent statistics released by the FSO (FSO 2022c) at the end of May 2022, the second (industry) and third (services) sectors are both affected by the difficulties in hiring personnel. The high-tech industry is also under strain, as are the hotel and restaurant industries. Healthcare, transportation, building, logistics, and even handicrafts in the construction industry are all impacted by scarcity. Even truck drivers are in high demand these days.

Authorities need to take measures now and not leave the people to just simply adapt to the situation. When harsh circumstances force people to adapt, this is a case of negative adaptation that harm society even more. Adaptation to poverty, lack of drinking water, and social exclusion happen all the time and everywhere. People should not be left prone to these matters in the future. This is an ethical responsibility today and in the future. Without strict regulations which are put in force, society will suffer even more from its current problems. The offenders will use the new means of technology to enhance their power. Otherwise, people will have to negatively adapt.

Ethical matters for the future

The emergence of the "filter bubble," the Internet's use of face recognition to assess user preferences, data protection, fraudulent movies (using deep fake), and security AI technology misuse and cyberspace are all factors that without a question, resulted in digitalization creating many new ethical concerns that are historically unique.

What happens when someone misuses AI? It is something beyond comprehension. For instance, the world's nations continue to disagree on whether tight regulations should be put in place to control the deployment of so-called "killer robots." After a week of discussions last spring at the UN in Geneva, the outcomes were mainly dismal (Raaflaub 2021). There are already a lot of remarks and recommendations available. However, a thorough examination of

84 pertinent papers by ETH Zurich revealed that no overarching ethical principles were present (Raaflaub 2021). It is uncertain if a universal regulation of AI can be established in the international environment given the stark variations in the fundamental ethical principles that govern various nations. The ETH's new AI department intends to depend on moral principles from Europe. This facility will house all the university's AI research. Alexander Ilic, the director, believes that humans should be the center of attention. A certain amount of duty also falls on the individual who creates something new. Therefore, we must influence this conversation and include European ideals in the creation of AI applications (Raaflaub 2021).

Data fairness

The most important word for data use is trust. Data mining techniques certainly have the potential to undermine trust and privacy. Numerous studies prove the loss of trust in institutions and companies (Hedewig-Mohr 13-Jan-22). There is an urgent need for a trust label so that users can restore their trust in data use. One of the promising solutions is “Data Fairness” as the Swiss Insights Association (Swiss-insights.ch) President Stefan Langenauer explains. He will present the newly developed Data Fairness label, which is intended to show that companies are committed to the transparent, comprehensible, and responsible handling of large amounts of data. On a website, a questionnaire is used to record the extent to which data sets, tools, or algorithms used contain possible bias - systematic errors towards certain population groups. The Data Fairness Label invites self-reflection. In addition, the results of the audits are to be discussed in a community, and finally, the owners of the label must adhere to certain guidelines.

5.2 Answers to Research Questions and Recommendations

This dissertation provided implicit answers to the research questions presented in the introduction in Box 1-1 (presented also below for clarity). Every chapter answered its related questions according to Table 1.1.

- **Question 1:** "What are the most challenges that face Society 5.0 in the dawn of mass technology dependence? What security breaches accompany the technological revolution in the future?"
- **Question 2:** "How will the future society impact the lives of individuals? How will technology affect various aspects of life?"
- **Question 3:** "What is the sustainable solution which reduces or negates the negative effects that accompany technology?"

The answer to research question 1 is summarized in Box 3-1. Research question 2 was addressed in two different chapters (see Table 1.1), and the answer is presented in Box 3-2 and Box 3-3. Research question 3 is addressed in chapter 4, and the summary of the answer is presented in Box 4-2.

There is no need to rewrite the summarized answers here again as they are easily accessible. However, concluding discussions and recommendations are useful.

Security breaches are countless. They take a more complex and digital form. The threats are not limited to cyber-bullying, cyber-blackmailing, social exclusion, bias in AI programming, spying, ethical problems, increased international security risks, unemployment, social division, and increased costs of living. Just like the steam engine changed society, so will technology. Societies are already internet dependent. The technology will continue to marsh and people will continue to adapt. Technology itself is not the problem. The threat is in the hands of those who develop this technology. The real world is for everyone, and so should the digital world. If a group of people whether of a race, religion, or a certain cultural background is not included in the development of technology, this does not mean that they can be overlooked or excluded.

Setting a limit to technology implementation is not realistic due to countless reasons such as competitiveness, productivity, global competition, social benefits, and increased life expectancy. Banning technology development, in general, is not possible, but banning the implementation for social and ethical concerns must be the case. People represented by Smart Sovereignty should decide these ethical and social borders, and that should not be left to governments and high-tech corporates.

Without Smart Sovereignty or an equivalent body, people will not have power over society's evolution. Big corporations will draw the headlines, and people will have to adapt and suffer the consequences. In societies built on capitalism, capitalism will only be enhanced and more emphasized when they transform into a smart society. Authoritarian societies will continue to remain the way they are. Profit-oriented societies will not change unless the change happens in the stage of development and implementation of technology.

Recommendations

The emergence of the future society is already happening. Everything is going digital and online. The importance of cyber-spaces is no less than the importance of physical spaces. People will need higher communication and IT skills to live up to and adapt to the new era. The world will witness increased automation and robotics use in most if not all aspects of life. Autonomous cars, robotics in healthcare, e-governance, and smart grids will be the mainstream in the future. Only with proper legislation, responsible application, and the correct implementation of Smart Sovereignty, future society will emerge in the favor of the public. The welfare and the prosperity of people will be the center of focus.

The future society is all about going digital and data is the base of the future society. The platforms which are the gate between the digital world and the real world need proper governance. Taking over these gates is the key to steering and influencing the social transition safely into the future. Integrating social values and ethics in the stage of development of modern technologies and avoiding any bias or racism for instance in the stage of programming will result in a smart society where most of the social problems will be easier to solve and address.

To achieve that the future smart society adheres to the principles of social ethics while placing the welfare of the people in focus, ethics must be respected especially in the development phases for AI, and in the design of the platforms (see Figure 3-4). Setting strict rules for the direction of technology development, and steering the development of innovations in favor of humans rather than corporations will enhance a promising smart society. Meanwhile, leaving the power in the hands of the few will only result in a smart society for some, and a harsh society for the many. The final recommendations are presented in Table 5.1.

Table 5.1: Recommendations

Recommendations for	
Government	• Launch the Smart Sovereignty initiative and set a reasonable timetable to complete and apply in society. Grant constant freedom and democracy during the development process. Include and train representatives from all the society in the Smart Sovereignty board. • Introduce a bill for basic unconditional income to be put into effect in the next decade. Review taxation laws and study the proposition of imposing robot taxations.
Legislators, ethics scholars, and thinkers	• review and rewrite the ethics of modern digital society and work together with legislators to promote these ethics throughout society
Researches	• Respect ethics, and make inclusive designs during tests that include all levels of society, races, religions, and minorities. Especially in medical experiments that aim to enhance AI and ML. • There are many gaps between theory and practice that need to be closed. Pay attention to the many out-of-date security-related definitions and concepts.
Computer engineers	• Adhere to ethics and always treat society as one unit to avoid social exclusion and division.
Cyber legislators	• Review cyber laws and create laws that protect a safe cyber. Readdress the laws regularly since technology changes constantly and cyber criminals discover always new loopholes in the system.
Politicians	• Put the interest of people and society above the political interest and conflicts.
Education	• Raise the awareness of smart society and the importance of security in digital spheres. Introduce subjects that address security matters at early stages of school education, particularly the risks of using social media among the young generation.

5.3 Limitations and Future Research

This subchapter presents the limitations of the dissertation before opening the door for future research topics.

5.3.1 Research Limitations

The security theory field is very broad which makes it difficult to cover every important matter and not miss anything. The challenges for society are countless, and one can write several books on only one simple matter. Therefore, the theory covered in this dissertation was somehow limited but in a way that serves the main purpose. Additionally, providing a proper definition for “Societal Security” requires more than the given space and time. If that definition was addressed as should be, the dissertation will certainly deviate from its path. Consequently, the author had to be content with the derived definition.

A similar limitation applies to the theory review of humankind and the perception of security. The necessary elements were successfully derived from the covered theory. However, one could write a dissertation on that matter alone, which is an interesting topic. Unfortunately, deeper insight into all human societies was not possible without doubling the amount of work and time needed to finish this dissertation. But that would not add any increased tangible benefit to the conclusion. In other words, despite the limited review of human societies, the summary is quite enough to serve the purpose of this dissertation.

The concept of Smart Sovereignty is well formulated and presented, but, it requires more research to become perfect as it is still in the early stages of its conceptualization, especially in terms of governance and control. However, this dissertation intends to bring this concept to life, and the mission is accomplished. Further steps of Smart Sovereignty development will be discussed in the following section.

The most challenging limitations were in the forecasting part in chapter 4. They were addressed properly in chapter 3.3.5.2. Moreover, converting aspects such as “quality of life” into numbers with enough variables that cover the necessary meanings is a big challenge. Unfortunately, there is a limitation to the availability and consistency of data on some occasions. Incomplete data for some variables. Additionally, the data of the FSO kept regularly

updating and changing even for recent entries which made it cumbersome to constantly remake the calculations. Nevertheless, no significant change in results was detected.

5.3.2 Future Research

This section makes recommendations regarding the theoretical research. This dissertation is the cornerstone and the starting point for Smart Sovereignty. There remains a lot to be investigated in this novel research field. Future research should seek to provide answers to sovereignty measurement and quantification problems. Another significant issue that will need to be investigated in the future is the development and applicability of sovereignty. The starting point is the rights and obligations of persons in a contemporary smart nation. Moreover, sovereignty governance is still at its cradle, and there is a huge potential for growth in this area. Additionally, security theory and security-related definitions need to be modernized and put into a digital context for smart societies. The definition of “Societal Security” remains open for revisiting and updating.

Future modern research on social responsibility and its relationship to technology evolution, also, robotics taxation, and the need for basic income is necessary to investigate for the sake of society and humanity. Society 5.0 will need many social studies such as individual behavior studies in smart society.

The forecasting approach is suitable for the future forecast with different points of interest for society. This can offer further insight into how Society 5.0 will evolve and can discover new weaknesses in the current system. The forecast could be applied to a wider range of industries and social attributes. Important elements for the success of Smart Sovereignty are the maturity and usability of Smart Sovereignty, especially with the increasing complexity of the future society. This matter needs further research. Additionally, finding out who the sovereign person is in the future Smart Society and what roles they play for sovereignty starting with the rights and duties of persons in a smart society is another important issue to research. Table 5.2 summarizes the suggested future research.

Table 5.2: Future Research

Research category	
Society 5.0	• Social studies on Society 5.0 are necessary to identify the characteristics of society and future social developments, needs, and movements. • Individual behavior, and groups' behavior in a smart society. • Studies on the rights and duties of a smart society are needed to establish revised laws that are suitable for a smart society. • Forecasting other aspects than security in Society 5.0 will help find more flaws in society and give enough time for proper intervention. • Follow up with research on Japan's Society 5.0 as case study to learn from the experience.
Security studies	• Studies on modern security concepts and particularly societal security are necessary to be up-to-date. • Closing the gap between theory and practice for smart societies. • Redefining a modern Maslow's Hierarchy of Needs for Society 5.0 since this hierarchy is out of date and needs to adapt to digital and smart context.
Smart Sovereignty	• Sovereignty measurements define a scale that can be used as a reference to the accepted level of sovereignty. • Sustainability and governance of Smart Sovereignty are still in their infancy and require deep research. • Characteristics of a sovereign individual and a sovereign society can be useful for different applications like security and psychology. • Studies on the factors of success and failure of Smart Sovereignty can help enhance sovereignty in the local society and export the experience to other countries.

6 Publication Bibliography

Acatech (2012): Cyber-Physical Systems: Driving Force for Innovations in Mobility, Health, Energy and Production: Springer Berlin Heidelberg. ISBN: 3642290892.

Aldabbas, Mohammad; Gstrein, Mario; Teufel, Stephanie (2015): Changing Energy Consumption Behaviour: Individuals' Responsibility and Government Role. In *Journal of Electronic Science and Technology* 13 (4), pp. 343–348. DOI: 10.11989/JEST.1674-862X.505263.

Aldabbas, Mohammad; Teufel, Bernd (2016): Human Aspects of Smart Technologies' Security. The Role of Human Failure. In *Journal of Electronic Science and Technology* 14 (4), pp. 311–318. DOI: 10.11989/JEST.1674-862X.605293.

Aldabbas, Mohammad; Teufel, Stephanie; Teufel, Bernd (2017): The importance of security culture for crowd energy systems. In : 2017 Information Security for South Africa (ISSA): IEEE. DOI: 10.1109/issa.2017.8251783.

Aldabbas, Mohammad; Teufel, Stephanie; Teufel, Bernd; Pasquier, Virgile (2020a): Smart Sovereignty: The Security Shield for Smart Society 5.0. In *IJDS* 11 (2), pp. 1619–1626. DOI: 10.20533/ijds.2040.2570.2020.0202.

Aldabbas, Mohammad; Teufel, Stephanie; Teufel, Bernd; Spycher, Jannick (2021): Forecasting the Quality of Life in a Future Smart Society, the Case of Switzerland. In *International Journal of Social Science and Humanity (IJSSH)* 12 (2), pp. 107–112. DOI: 10.18178/ijssh.2022.12.2.1075.

Aldabbas, Mohammad; Xie, Xuan; Teufel, Stephanie; Teufel, Bernd (2020b): Future Security Challenges for Smart Societies: Overview from Technical and Societal Perspectives. In : International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 103–111. DOI: 10.1109/ICSGCE49177.2020.9275630.

AlHogail, A; Mirza, A: Information security culture: A definition and a literature review. In *In 2014 World Congress on Computer Applications and Information Systems (WCCAIS).*, pp. 1–7. DOI: 10.1109/WCCAIS.2014.6916579.

AlHogail, Areej (2018): Improving IoT Technology Adoption through Improving Consumer Trust. In *Technologies* 6 (3), p. 64. DOI: 10.3390/technologies6030064.

Allam, Zaheer (2020): Privatization and privacy in the digital city. In : Cities and the digital revolution: Springer., pp. 85–106. ISBN: 978-3-030-29800-5.

Amankwa, E; Loock, M; Kritzinger, E: A conceptual analysis of information security education, information security training and information security awareness definitions. In *In The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).*, pp. 248–252. DOI: 10.1109/ICITST.2014.7038814.

Amazon Forecast (2021): Exponential Smoothing (ETS) Algorithm - Amazon Forecast. Available online at https://docs.aws.amazon.com/forecast/latest/dg/aws-forecast-recipe-ets.html, updated on 07-Jun-21, checked on 07-Jun-21.

Amundrud, Øystein; Aven, Terje; Flage, Roger (2017): How the definition of security risk can be made compatible with safety definitions. In *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 231 (3), pp. 286–294. DOI: 10.1177/1748006X17699145.

Anderson, James M. (2003): Why we need a new definition of information security. In *Computers & Security* 22 (4), pp. 308–313. DOI: 10.1016/S0167-4048(03)00407-3.

Ang, B. W.; Choong, W. L.; Ng, T. S. (2014): Energy security: Definitions, dimensions and indexes. In *Renewable and Sustainable Energy Reviews* 42, pp. 1077–1093. DOI: 10.1016/J.RSER.2014.10.064.

Aquinas, T. (2002): Political Writings, ed. RW Dyson. ISBN: 978-0521375955.

Arute, Frank; Arya, Kunal; Babbush, Ryan; Bacon, Dave; Bardin, Joseph C.; Barends, Rami et al. (2019): Quantum supremacy using a programmable superconducting processor. In *Nature* 574 (7779), pp. 505–510. DOI: 10.1038/s41586-019-1666-5.

Ashley, Richard K. (1984): The Poverty of Neorealism. In *International organization* 38 (2), pp. 225–286. DOI: 10.1017/s0020818300026709.

Atella, Vincenzo; Piano Mortari, Andrea; Kopinska, Joanna; Belotti, Federico; Lapi, Francesco; Cricelli, Claudio; Fontana, Luigi (2019): Trends in age-related disease burden and healthcare utilization. In *Aging cell* 18 (1). DOI: 10.1111/acel.12861.

Atkinson, Anthony B. (2016): Inequality: What can be done. In *Practice* 40 (2), pp. 289–292. DOI: 10.3326/fintp.40.2.6.

Aven, Terje (2007): A unified framework for risk and vulnerability analysis covering both safety and security. In *Reliability engineering & System safety* 92 (6), pp. 745–754. DOI: 10.1016/j.ress.2006.03.008.

Awad, Edmond; Dsouza, Sohan; Kim, Richard; Schulz, Jonathan; Henrich, Joseph; Shariff, Azim et al. (2018): The Moral Machine Experiment. In *Nature* 563 (7729), pp. 59–64. DOI: 10.1038/s41586-018-0637-6.

Baker, Matthew J. (2003): An Equilibrium Conflict Model of Land Tenure in Hunter-Gatherer Societies. In *Journal of Political Economy* 111 (1), pp. 124–173. DOI: 10.1086/344800.

Baldwin, David A. (1997): The Concept of Security. In *Review of International Studies* 23(1), pp. 5–26. DOI: 10.1017/S0260210597000053.

Bar-Cohen, Yoseph (2005): Biomimetics: mimicking and inspired-by biology. In *Smart Structures and Materials 2005: Electroactive Polymer Actuators and Devices (EAPAD)* 5759 (02), pp. 1–8. DOI: 10.1117/12.597436.

Barkin, J. Samuel; Cronin, Bruce (1994): The state and the nation: changing norms and the rules of sovereignty in international relations. In *International organization* 48 (1), pp. 107–130. DOI: 10.1017/s0020818300000837.

Barzilay, Menny (2013): A simple definition of cybersecurity: ISACA. Available online at https://www.isaca.org/resources/news-and-trends/isaca-now-blog.

Bauer, Andreas (2019): Sicherheitsstrategie in Unternehmen. Eine theoretische Übersicht. Bachelor Thesis. University of Fribourg. (iimt) international institute of management in technology.

Bauman, Zygmunt; Bigo, Didier; Esteves, Paulo; Guild, Elspeth; Jabri, Vivienne; Lyon, David; Walker, Rob B. J. (2014): After Snowden: Rethinking the impact of surveillance. In *International political sociology* 8 (2), pp. 121–144. DOI: 10.1111/ips.12048.

Bayer, Joseph B.; Triệu, Penny; Ellison, Nicole B. (2020): Social Media Elements, Ecologies, and Effects. In *Annual review of psychology* 71, pp. 471–497. DOI: 10.1146/annurev-psych-010419-050944.

Bellwood, Peter (2005): First Farmers. The Origins of Agricultural Societies. 5 ed. Malden, Oxford, Carlton: Blackwell. ISBN: 9780631205661.

Bender, Barbara (1978): Gatherer-hunter to farmer: A social perspective. In *World Archaeology* 10 (2), pp. 204–222. DOI: 10.1080/00438243.1978.9979731.

Bentley, R. Alexander; O'Brien, Michael J. (2017): The acceleration of cultural change: From ancestors to algorithms: MIT Press. ISBN: 0262036959.

Bernaert, Arnaud; Akpakwu, Emmanuel (Eds.) (2018): Four ways AI can make healthcare more efficient and affordable. In World Economic Forum. weforum.org/agenda/2018/05/four-ways-ai-is-bringing-down-the-cost-ofhealthcare. World Economic Forum. weforum.org/agenda/2018/05/four-ways-ai-is-bringing-down-the-cost-ofhealthcare.

Besson, Samantha (2011): Sovereignty, international law and democracy. In *European Journal of International Law* 22 (2), pp. 373–387. DOI: 10.1093/ejil/chr029.

Bican, Peter M.; Brem, Alexander (2020): Digital business model, digital transformation, digital entrepreneurship: Is there a sustainable "digital"? In *Sustainability* 12 (13), p. 5239. DOI: 10.3390/su12135239.

Binford, Lewis R. (1980): Willow Smoke and Dogs' Tails: Hunter-Gatherer Settlement Systems and Archaeological Site Formation. In *Am. antiq.* 45 (1), pp. 4–20. DOI: 10.2307/279653.

Bishop, Matt (2003): What is computer security? In *IEEE Security & Privacy* 1 (1), pp. 67–69. DOI: 10.1109/MSECP.2003.1176998.

Bloomberg (2015): 7 phases of a data life cycle | Bloomberg Professional Services. Edited by Bloomberg Professional Services. Available online at https://www.bloomberg.com/professional/blog/7-phases-of-a-data-life-cycle/, updated on 21-May-20, checked on 13-Oct-20.

Bocquet-Appel, Jean-Pierre (2011): When the world's population took off: the springboard of the Neolithic Demographic Transition. In *Science (New York, N.Y.)* 333 (6042), pp. 560–561. DOI: 10.1126/science.1208880.

Bohi, Douglas R.; Toman, Michael A.; Margaret, A. (1996): The Economics of Energy Security. ISBN: 978-94-010-7305-9.

Bösch, Patrick M. (2018): Autonomous Vehicles-The next Revolution in Mobility. Doctoral Thesis. ETH Zurich.

Box, George E. P.; Jenkins, Gwilym M.; Reinsel, Gregory C.; Ljung, Greta M. (2016): Time series analysis. Forecasting and control / George E.P. Box, Gwilym M. Jenkins, Gregory C. Reinsel, Greta M. Ljung. Fifth edition. Hoboken, New Jersey: Wiley (Wiley series in probability and statistics. ISBN: 9781118675021.

Braithwaite, Jeffrey (2005): Hunter-gatherer human nature and health system safety: an evolutionary cleft stick? In *International journal for quality in health care : journal of the International Society for Quality in Health Care* 17 (6), pp. 541–545. DOI: 10.1093/intqhc/mzi060.

Braithwaite, Tom (2020): Prospering in the pandemic: the top 100 companies. In *Financial Times*, 6/19/2020. Available online at https://www.ft.com/content/844ed28c-8074-4856-bde0-20f3bf4cd8f0, checked on 11/11/2020.

Brandtzaeg, Petter Bae; Følstad, Asbjørn (2018): Chatbots: changing user needs and motivations. In *Interactions* 25 (5), pp. 38–43. DOI: 10.1145/3236669.

Brendler, Pavel (2020): Why hasn't Social Security changed since 1977? In *Review of Economic Dynamics* 36, pp. 134–157. DOI: 10.1016/j.red.2019.09.001.

Brennen, J. (2018): An industry-led debate: How UK media cover artificial intelligence.

Briscoe, Erica; Fairbanks, James (2020): Artificial Scientific Intelligence and its Impact on National Security and Foreign Policy. In *Orbis* 64 (4), pp. 544–554. DOI: 10.1016/j.orbis.2020.08.004.

Brodbeck, Karl-Heinz (2007): ABC der Wissenschaftstheorie für Betriebswirte. Available online at Retrieved from Hochschule für Angewandte Wissenschaften Würzburg Schweinfurt https://opus4.kobv.de/opus4-fhws/frontdoor/index/index/docId/77.

Brogårdh, Torgny (2007): Present and future robot control development—An industrial perspective. In *Annual Reviews in Control* 31 (1), pp. 69–79. DOI: 10.1016/j.arcontrol.2007.01.002.

Brooks, David J. (2010): What is security: Definition through knowledge categorization. In *Security Journal* 23 (3), pp. 225–239. DOI: 10.1057/sj.2008.18.

Brownlee, Jason (2017): How to Decompose Time Series Data into Trend and Seasonality. Available online at https://machinelearningmastery.com/decompose-time-series-data-trend-seasonality/, updated on 29-Jan-17, checked on 05-Aug-22.

Brühwiler, Claudia Franziska; Egli, Patricia; Sánchez, Yvette (2019): The ICRC at a crossroads: Swiss roots—international outlook. In *Int J Humanitarian Action* 4 (1), pp. 1–17. DOI: 10.1186/s41018-019-0060-0.

Budnitsky, Stanislav; Jia, Lianrui (2018): Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. In *European Journal of Cultural Studies* 21 (5), pp. 594–613. DOI: 10.1177/1367549417751151.

Bughin, Jacques; Hazan, Eric; Ramaswamy, Sree; Chui, Michael; Allas, Tera; Dahlstrom, Peter et al. (2017): Artificial intelligence: The next digital frontier? In *Mckinsey Global Institute: New York, NY, USA*, 1–80. Available online at https://www.calpers.ca.gov/docs/board-agendas/201801/full/day1/06-technology-background.pdf.

Burgess, J. P.; Mouhleb, N. (2007): Societal Security. Definitions and Scope for the Norwegian Setting ,.2). ISBN: 978-82-7288-247-0.

Burgess, J. Peter (2010): The Routledge handbook of new security studies. London, New York: Routledge (Routledge handbooks. ISBN: 9781135166199.

Burns, Alan; McDermid, John; Dobson, J. (1992): On the meaning of safety and security. In *The Computer Journal* 35 (1), pp. 3–15. DOI: 10.1093/comjnl/35.1.3.

Bush, George W. (2009): The National Security Strategy of the United States of America: Morgan James Pub. ISBN: 9781600375873.

Bynum, T. (2015): Computer and information ethics. In EN Zalta (ed.), The Stanford encyclopedia of philosophy. Available online at https://stanford.library.sydney.edu.au/archives/fall2015/entries/ethics-computer/.

Cabinet Office (2018): Society 5.0. Edited by Cabinet Office, Government of Japan. Available online at https://www8.cao.go.jp/cstp/english/society5_0/index.html, updated on 20-Nov-18, checked on 25-Jun-19.

Cai, Z. Q; Zhao, J. B; Li, Y; Si, S. B; Ni, M. N (2015): Information security evaluation of system based on Bayesian network. In : 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 315–319. DOI: 10.1109/IEEM.2015.7385659.

Calp, M. Hanefi; Bütüner, Resul (2022): Society 5.0: Effective technology for a smart society. In Aboul Ella Hassanien, Jyotir Moy Chatterjee, Vishal Jain (Eds.): Artificial intelligence and industry 4.0. Amsterdam: Academic Press (Intelligent data centric systems), pp. 175–194. ISBN: 9780323884686. DOI: 10.1016/B978-0-323-88468-6.00006-1.

Calvin, Nathan; Leung, Jade (2020): Who owns artificial intelligence? A preliminary analysis of corporate intellectual property strategies and why they matter. In *Future of Humanity Institute*. Available online at https://www.fhi.ox.ac.uk/wp-content/uploads/Patents_-FHI-Working-Paper-Final-.pdf.

Cambridge (2020): SECURITY OF TENURE | meaning in the Cambridge English Dictionary. Available online at https://dictionary.cambridge.org/dictionary/english/security-of-tenure, updated on 21-Sep-20, checked on 21-Sep-20.

Campbell, Bruce (2005): The agrarian problem in the early fourteenth century. In *Past & Present* 188 (1), pp. 3–70. DOI: 10.1093/pastj/gti017.

Capurro, Rafael (2009): Digital ethics. In *Global Forum on Civilization and Peace. Seoul*, pp. 207–216.

Caron, Xavier; Bosua, Rachelle; Maynard, Sean B.; Ahmad, Atif (2016): The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. In *Computer Law & Security Review* 32 (1), pp. 4–15. DOI: 10.1016/j.clsr.2015.12.001.

Cath, Corinne (2018): Governing artificial intelligence: ethical, legal and technical opportunities and challenges. In *Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences* 376(2133). DOI: 10.1098/rsta.2018.0080.

Cengiz, Aslihan Banu; Kalem, Guler; Boluk, Pinar Sarisaray (2022): The Effect of Social Media User Behaviors on Security and Privacy Threats. In *IEEE Access*. DOI: 10.1109/ACCESS.2022.3177652.

CERN (2020): Computer Security: Blackmailing Enterprises: You are Patient Zero. Available online at https://home.cern/news/news/computing/computer-security-blackmailing-enterprises-you-are-patient-zero, updated on 01-Jul-22, checked on 01-Jul-22.

Chambers, John C.; Mullick, Satinder K.; Smith, Donald D. (1971): How to Choose the Right Forecasting Technique. Harvard Business Review. Available online at https://hbr.org/1971/07/how-to-choose-the-right-forecasting-technique, updated on 01-Aug-14, checked on 08-Jun-21.

Chen, Deyan; Zhao, Hong (2012): Data security and privacy protection issues in cloud computing. In : International Conference on Computer Science and Electronics Engineering: IEEE (1), pp. 647–651. ISBN: 0769546471. DOI: 10.1109/ICCSEE.2012.193.

Chester, Lynne (2010): Conceptualising energy security and making explicit its polysemic nature. In *Energy policy* 38 (2), pp. 887–895. DOI: 10.1016/j.enpol.2009.10.039.

Chesterman, Simon (2001): Just War or Just Peace?: International Law and Humanitarian Intervention. Available online at https://scholar.google.com/citations?user=vipjkwiaaaaj&hl=en&oi=sra. ISBN: 978-0199257997.

Choong, W. L.; Ang, B. W.; Ng, T. S. (2014): Going green and energy security. In : International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE), pp. 1–8. Available online at https://ieeexplore.ieee.org/abstract/document/6828948.

Christen, Markus (2021): KI löst unsere Grundprobleme nicht. Edited by higgs. Available online at https://www.higgs.ch/ki-loest-unsere-grundprobleme-nicht/31492/, updated on 3/18/2021, checked on 3/18/2021.

Chuang, Yih-chyi; Thomas, Simona (2010): China and the world economy. China's economic rise after three decades of reform. Berlin, Münster: Lit (Berliner China-Hefte,.Vol. 37). ISBN: 9783643999221.

Clark, Helen; Wu, Hongbo (2016): Sustainable Development Goals: 17 Goals to Transform our World. In *Furthering the Work of the United Nations; UN: New York, NY, USA*, pp. 36–54. Available online at https://www.un.org/en/exhibits/page/sdgs-17-goals-transform-world.

Coffey, Dan; Thornley, Carole (2006): Automation, motivation and lean production reconsidered. In *Assembly Automation* 26(2), pp. 98–103. DOI: 10.1108/01445150610658068.

Collard, G; Ducroquet, S; Disson, E; Talens, G (2017): A definition of Information Security Classification in cybersecurity context. In : 2017 11th International Conference on Research Challenges in Information Science (RCIS), pp. 77–82. Available online at https://doi.org/10.1109/RCIS.2017.7956520. DOI: 10.1109/RCIS.2017.7956520.

Conlon, Justin (2004): Sovereignty vs. Human Rights or Sovereignty and Human Rights? In *Race & Class* 46 (1), pp. 75–100. DOI: 10.1177/0306396804045516.

Craig, Kevin; Sadovykh, Valeria (Eds.) (2022): Perceived Social Media Bias, Social Identity Threat, and Conspiracy Theory Ideation During the COVID-19 Pandemic: ISBN: 0998133159. Available online at http://hdl.handle.net/10125/80066.

Craigen, Dan; Diakun-Thibault, Nadia; Purse, Randy (2014): Defining cybersecurity. In *Technology Innovation Management Review* 4 (10), pp. 13–21. DOI: 10.22215/timreview/835.

Crawford, Kate; Calo, Ryan (2016): There is a blind spot in AI research. In *Nature News* 538 (7625), p. 311. DOI: 10.1038/538311a.

Cukurova, Mutlu; Kent, Carmel; Luckin, Rosemary (2019): Artificial intelligence and multimodal data in the service of human decision-making: A case study in debate tutoring. In *British Journal of Educational Technology* 50 (6), pp. 3032–3046. DOI: 10.1111/bjet.12829.

Culnan, Mary J.; Armstrong, Pamela K. (1999): Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. In *Organization science* 10 (1), pp. 104–115. DOI: 10.1287/orsc.10.1.104.

Da Costa Tavares, Maria Conceição; do Carmo Azevedo, Graça Maria (2020): Society 5.0 as a contribution to the sustainable development report. In : International Conference on Tourism, Technology and Systems: Springer, pp. 49–63. DOI: 10.1007/978-981-33-4256-9_5.

Davidow, Moshe (2018): Value creation and efficiency: incompatible or inseparable? In *Journal of creating value* 4 (1), pp. 123–131. DOI: 10.1177/2394964318768904.

Deguchi, Atsushi; Hirai, Chiaki; Matsuoka, Hideyuki; Nakano, Taku; Oshima, Kohei; Tai, Mitsuharu; Tani, Shigeyuki: What Is Society 5.0? In, pp. 1–23.

Deibert, Ronald J. (2018): Toward a Human-Centric Approach to Cybersecurity. In *Ethics int. aff.* 32 (4), pp. 411–424. DOI: 10.1017/S0892679418000618.

Delang, Claudio O. (2006): The role of wild food plants in poverty alleviation and biodiversity conservation in tropical countries. In *Progress in Development Studies* 6 (4), pp. 275–286. DOI: 10.1191/1464993406ps143oa.

Domingos, Pedro (2015): The master algorithm: How the quest for the ultimate learning machine will remake our world: Basic Books. ISBN: 0465061923.

Doncaster, C. Patrick (2019): Timetable of human evolution and cultural development. University of Southampton. Available online at http://www.southampton.ac.uk/~cpd/history.html, updated on 07-Feb-19, checked on 19-Jul-19.

Ducrot, Vincent (2019): Herausforderungen für die Mobilität von morgen. Presentation as part of the lecture "Frinourg von morgen", 2019.

Dufva, Tomi; Dufva, Mikko (2019): Grasping the future of the digital society. In *Futures* 107, pp. 17–28. DOI: 10.1016/j.futures.2018.11.001.

Duguid, Margaret (2012): The Importance of Medication Reconciliation for Patients and Practitioners. In *Australian Prescriber* 35 (1), pp. 15–19. DOI: 10.18773/austprescr.2012.065.

Düwell, Marcus; Hübenthal, Christoph; Werner, Micha H. (2011): Handbuch Ethik. 3rd ed. Stuttgart (Springer eBook Collection. ISBN: 9783476051929.

Eames, David Peter; Moffett, Jonathan (1999): The Integration of Safety and Security Requirements. In : International Conference on Computer Safety, Reliability, and Security: Springer, pp. 468–480. DOI: 10.1007/3-540-48249-0_40.

Elenev, Vadim; Landvoigt, Tim; van Nieuwerburgh, Stijn (2020): Can the Covid Bailouts Save the Economy? National Bureau of Economic Research. DOI: 10.3386/w27207.

Ember, Carol R. (1978): Myths about Hunter-Gatherers. In *Ethnology* 17 (4), p. 439. DOI: 10.2307/3773193.

European Commission (2001): Green Paper: Towards a European strategy for the security of energy supply: Office for Official Publications of the European Communities. ISBN: 9289403195.

European Commission (2020): The Digital Economy and Society Index (DESI). Available online at https://digital-strategy.ec.europa.eu/en/policies/desi, updated on 09-Aug-21, checked on 09-Aug-21.

European Commission (2021): Shaping Europe's digital future. expert group on AI. Available online at https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai, updated on 4/5/2021, checked on 4/5/2021.

European Union (2018): General Data Protection Regulation (GDPR) – Official Legal Text. Available online at https://gdpr-info.eu/, updated on 2/9/2019, checked on 10/11/2020.

Evans, Gareth (2008): The Responsibility to Protect: An Idea Whose Time Has Come… and Gone? In *International relations* 22 (3), pp. 283–298. DOI: 10.1177/0047117808094173.

FAO (2001): The State of Food and Agriculture 2001: Food & Agriculture Org ,.33). ISBN: 925104600X.

Feng, Bo; Ye, Qiwen (2021): Operations management of smart logistics: A literature review and future research. In *Front. Eng. Manag.* 8 (3), pp. 344–355. DOI: 10.1007/s42524-021-0156-2.

Finnemore, Martha (2003): The Purpose of Intervention: Changing Beliefs about the Use of Force: Cornell University Press, Ithaca, NY. ISBN: 9788170492054.

Floridi, Luciano (2016a): Faultless responsibility: On the nature and allocation of moral responsibility for distributed moral actions. In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083), pp. 1–13. DOI: 10.1098/rsta.2016.0112.

Floridi, Luciano (2016b): Mature Information Societies—a Matter of Expectations. In *Philosophy & Technology* 29 (1), pp. 1–4. DOI: 10.1007/s13347-016-0214-6.

Floridi, Luciano (2018): Soft Ethics and the Governance of the Digital. In *Philosophy & Technology* 31 (1), pp. 1–8. DOI: 10.1007/s13347-018-0303-9.

Floridi, Luciano; Taddeo, Mariarosaria (2016): What is data ethics? In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2083). DOI: 10.1098/rsta.2016.0360.

Ford, Martin (2018): Architects of Intelligence: The truth about AI from the people building it: Packt Publishing Ltd. ISBN: 178913126X.

Franceschini, Gianluca; Mason, Elena Jane; Orlandi, Armando; D'Archi, Sabatino; Sanchez, Alejandro Martin; Masetti, Riccardo (2021): How will artificial intelligence impact breast cancer research efficiency? In *Expert Review of Anticancer Therapy* 21 (10), pp. 1067–1070. DOI: 10.1080/14737140.2021.1951240.

Freddi, Daniela (2018): Digitalisation and employment in manufacturing. In *AI & Soc* 33 (3), pp. 393–403. DOI: 10.1007/s00146-017-0740-5.

Freedom Online Coalition Working Group (2015): Recommendations for Human Rights Based Approaches to Cybersecurity, Freedom Online Coalition. Access date: 02.12.20. Available online at http://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf, updated on 02-Dec-20, checked on 02-Dec-20.

Freeman, Jacob; Anderies, John M. (2015): The socioecology of hunter–gatherer territory size. In *Journal of Anthropological Archaeology* 39, pp. 110–123. DOI: 10.1016/j.jaa.2015.03.002.

Frei, Regina; McWilliam, Richard; Derrick, Benjamin; Purvis, Alan; Tiwari, Asutosh; Di Marzo Serugendo, Giovanna (2013): Self-healing and self-repairing technologies. In *The International Journal of Advanced Manufacturing Technology* 69 (5), pp. 1033–1061. DOI: 10.1007/s00170-013-5070-2.

Freitas, Robert A. (1999): Nanomedicine, volume I: basic capabilities: Landes Bioscience Georgetown, TX. ISBN: 9781570596803.

Frost, Jim (2019): Regression analysis: An intuitive guide for using and interpreting linear models: Statisics By Jim Publishing. ISBN: 1735431184.

FSO (2021a): ILO unemployed. Available online at https://www.bfs.admin.ch/bfs/en/home/statistics/work-income/unemployment-

underemployment-vacancies/ilo-unemployed.html, updated on 06-May-21, checked on 06-May-21.

FSO (2021b): Indexation. Available online at https://www.bfs.admin.ch/bfs/en/home/statistics/prices/consumer-price-index/indexierung.html, updated on 04-Aug-22, checked on 04-Aug-22.

FSO (2021c): Unemployment Statistics (ILO-based). Available online at https://www.bfs.admin.ch/bfs/en/home/statistics/work-income/surveys/els-ilo.html, updated on 06-May-21, checked on 06-May-21.

FSO (2022a): Consumer Price Index (CPI): basket and weights - 2021 | Diagram | Federal Statistical Office. Available online at https://www.bfs.admin.ch/bfs/en/home/statistics/catalogues-databases/graphs.assetdetail.15944831.html, updated on 12-Feb-21, checked on 04-Aug-22.

FSO (2022b): Consumer Prices. Available online at https://www.bfs.admin.ch/bfs/en/home/statistics/prices/consumer-price-index.html, updated on 04-Aug-22, checked on 04-Aug-22.

FSO (2022c): Starker Anstieg der Beschäftigung und der offenen Stellen in der Schweiz im 1. Quartal 2022 - Beschäftigungsbarometer im 1. Quartal 2022 | Medienmitteilung | Bundesamt für Statistik. Available online at https://www.bfs.admin.ch/bfs/de/home/aktuell/medienmitteilungen.assetdetail.22604245.html, updated on 30-May-22, checked on 09-Aug-22.

Fujiyoshi, Hironobu; Hirakawa, Tsubasa; Yamashita, Takayoshi (2019): Deep learning-based image recognition for autonomous driving. In *IATSS research* 43 (4), pp. 244–252. DOI: 10.1016/j.iatssr.2019.11.008.

Fukuyama, Mayumi (2018): Society 5.0: Aiming for a New Human-Centered Society. In *Japan SPOTLIGHT*, pp. 47–50. Available online at https://www.jef.or.jp/journal/pdf/220th_Special_Article_02.pdf.

Gallacher, Guillermo; Hossain, Iqbal (2020): Remote work and employment dynamics under COVID-19: Evidence from Canada. In *Canadian Public Policy* 46 (S1), S44-S54. DOI: 10.3138/cpp.2020-026.

Gat, Azar (2000): The Human Motivational Complex: Evolutionary Theory and the Causes of Hunter-Gatherer Fighting, Part II. Proximate, Subordinate, and Derivative Causes. In *Anthropological Quarterly* 73 (2), pp. 74–88. Available online at http://www.jstor.org/stable/3317188.

Gcaza, Noluxolo; von Solms, Rossouw; Grobler, Marthie M.; van Vuuren, Joey Jansen (2017): A general morphological analysis: Delineating a cyber-security culture. In *Information and Computer Security* 25 (3), pp. 259–278. DOI: 10.1108/ICS-12-2015-0046.

Geers, Kenneth (2010): Cyber Weapons Convention. In *Computer Law & Security Review* 26 (5), pp. 547–551. DOI: 10.1016/j.clsr.2010.07.005.

George, Richard (2003): Tourist's perceptions of safety and security while visiting Cape Town. In *Tourism Management* 24 (5), pp. 575–585. DOI: 10.1016/S0261-5177(03)00003-7.

George, Richard; Booyens, Irma (2014): Township tourism demand: Tourists' perceptions of safety and security. In : Urban Forum: Springer (25), pp. 449–467. ISBN: 1015-3802. DOI: 10.1007/s12132-014-9228-2.

Gest, Justin (2016): The new minority: White working class politics in an age of immigration and inequality: Oxford University Press. ISBN: 0190632550.

Gibney, Elizabeth (2020): The battle for ethical AI at the world's biggest machine-learning conference. In *Nature* 577 (7792), p. 609. DOI: 10.1038/d41586-020-00160-y.

Gill, G. K.; Gill, T. k.; Singh, R. (2015): Energy security - the issue of present time. In : 2015 IEEE 10th Conference on Industrial Electronics and Applications (ICIEA), pp. 2065–2068. DOI: 10.1109/ICIEA.2015.7334455.

Gilpin, Robert (1981): War and Change in World Politics. Cambridge: Cambridge University Press. ISBN: 9780511664267.

Giumetti, Gary W.; Kowalski, Robin M. (2022): Cyberbullying via social media and well-being. In *Current Opinion in Psychology*, p. 101314. DOI: 10.1016/j.copsyc.2022.101314.

Glanville, Luke (2013): The Myth of "Traditional" Sovereignty. In *Int Stud Q* 57 (1), pp. 79–90. DOI: 10.1111/isqu.12004.

Glasius, Marlies (2018): What authoritarianism is… and is not: a practice perspective. In *International Affairs* 94 (3), pp. 515–533. DOI: 10.1093/ia/iiy060.

Godfray, H. Charles J.; Beddington, John R.; Crute, Ian R.; Haddad, Lawrence; Lawrence, David; Muir, James F. et al. (2010): Food security: the challenge of feeding 9 billion people. In *Science* 327 (5967), pp. 812–818. DOI: 10.1126/science.1185383.

Goldemberg, Jose (2000): Energy and the challenge of sustainability. In *World Energy Assessment: United Nations Publications*. Available online at http://www.pnud.org/content/dam/aplaws/publication/en/publications/environment-energy/www-ee-library/sustainable-energy/world-energy-assessment-energy-and-the-challenge-of-sustainability/World%20Energy%20Assessment-2000.pdf.

Goldsmith, Jack L. (2017): The Internet and the Abiding Significance of Territorial Sovereignty. In PaulSchiff Berman (Ed.): The Globalization of International Law. First edition: Routledge, pp. 79–96. ISBN: 9781315086392. DOI: 10.4324/9781315086392-8.

Golliez, André (2022): Data Sovereignty. Swiss Academy of Engineering Sciences (SATW). Available online at https://www.satw.ch/en/technology-outlook-2021/significance-of-the-technologies-for-switzerland/datensouveraenitaet.

González Páramo, José Manuel (2017): Financial innovation in the digital age: Challenges for regulation and supervision. In *Revista de estabilidad financiera. Nº 32 (mayo 2017), p. 9-37*. Available online at https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/17/MAYO%202017/Articulo_GonzalezParamo.pdf.

Graetz, Georg; Michaels, Guy (2017): Is modern technology responsible for jobless recoveries? In *American Economic Review* 107 (5), pp. 168–173. DOI: 10.1257/aer.p20171100.

Gräf, Eike; Lahmann, Henning; Otto, Philipp (2018): Die Stärkung der digitalen Souveränität. Access date: 10.12.2021. Available online at https://www.divsi.de/wp-content/uploads/2018/05/DIVSI-Themenpapier-Digitale-Souveraenitaet.pdf.

Granier, Benoit; Kudo, Hiroko (2016): How are citizens involved in smart cities? Analysing citizen participation in Japanese``Smart Communities''. In *Information Polity* 21 (1), pp. 61–76. DOI: 10.3233/IP-150367.

Greene, Daniel; Hoffmann, Anna Lauren; Stark, Luke (2019): Better, nicer, clearer, fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning. ISBN: 0998133124.

Grizold, Anton (1994): The concept of national security in the contemporary world. In *International Journal on World Peace*, pp. 37–53. Available online at https://www.jstor.org/stable/20751984.

Gross, Rainer; Schoeneberger, Hans; Pfeifer, Hans; Preuss, Hans-Joachim (2000): The four dimensions of food and nutrition security: definitions and concepts. In *Nutrition and Food Security* 20 (20), pp. 20–25. Available online at http://www.fao.org/elearning/course/FA/en/pdf/P-01_RG_Concept.pdf.

Grotenhuis, René (2016): Nation-building: Sovereignty and citizenship. In : Nation-Building as Necessary Effort in Fragile States: Amsterdam University Press, pp. 59–72. Available online at https://www.jstor.org/stable/j.ctt1gr7d8r.7, checked on 11/4/2019. ISBN: 978-94-6298-219-2. DOI: 10.2307/j.ctt1gr7d8r.7.

Gstrein, Mario; Hertig, Yves; Teufel, Bernd; Teufel, Stephanie (2016): Crowd Energy – das Kooperationskonzept für Smart Cities. In Andreas Meier, Edy Portmann (Eds.): Smart City. Strategie, Governance und Projekte / Andreas Meier, Edy Portmann, Herausgeber. Wiesbaden, Germany: Springer Vieweg (Edition HMD), pp. 277–303. ISBN: 978-3-658-15616-9. DOI: 10.1007/978-3-658-15617-6_14.

Guitton, Matthieu J. (2022): Sovereignty in the age of technology: Challenges and Opportunities. In *Computers in Human Behavior* 134, p. 107331. DOI: 10.1016/j.chb.2022.107331.

Gul, M. Junaid; Subramanian, Barathi; Paul, Anand; Kim, Jeonghong (2021): Blockchain for public health care in smart society. In *Microprocessors and Microsystems* 80, p. 103524. DOI: 10.1016/j.micpro.2020.103524.

Haanaes, Knut (2016): Why all businesses should embrace sustainability. Available online at https://www.imd.org/contentassets/44380898a141424abb873f8774127bc4/tc082-16_why-all-businesses-should-embrace-sustainability_haanaes-2022-update-version.pdf, checked on 10/03/22.

Haider, Muzmmal; Ashraf, Sharjeel; Yasmin, Farhana (2022): A Critical Discourse Analysis of Cyberbullying Among University Students in Pakistan. In *International Journal of Linguistics and Culture* 3 (1), pp. 95–109. Available online at https://www.internationaljournalofspecialeducation.com/submission/index.php/ijse/article/view/1467/1164.

Halbert, Debora (2016): Intellectual property theft and national security: Agendas and assumptions. In *The Information Society* 32 (4), pp. 256–268. DOI: 10.1080/01972243.2016.1177762.

Hall, Kat (2017): Infosec guru Schneier: Govts will intervene to regulate Internet of Sh!t, 6/8/2017. Available online at https://www.theregister.com/2017/06/08/governments_will_intervene_insecure_iot/, checked on 11/13/2020.

Hamilton, Marcus J.; Milne, Bruce T.; Walker, Robert S.; Brown, James H. (2007a): Nonlinear scaling of space use in human hunter-gatherers. In *Proceedings of the National Academy of Sciences of the United States of America* 104 (11), pp. 4765–4769. DOI: 10.1073/pnas.0611197104.

Hamilton, Marcus J.; Milne, Bruce T.; Walker, Robert S.; Burger, Oskar; Brown, James H. (2007b): The complex structure of hunter-gatherer social networks. In *Proceedings. Biological sciences* 274 (1622), pp. 2195–2202. DOI: 10.1098/rspb.2007.0564.

Hanly, Ken (2019): Amazon uses Artificial Intelligence to fire warehouse workers. Available online at http://www.digitaljournal.com/tech-and-science/technology/amazon-uses-artificial-intelligence-to-fire-warehouse-workers/article/548594, updated on 3/19/2021, checked on 3/19/2021.

Hast, Susanna (2016): Spheres of Influence in International Relations. History, Theory and Politics. 1st ed. London: Taylor and Francis. Available online at https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=4468707. ISBN: 9781317051312.

Heaven, Douglas (2019): Why deep-learning AIs are so easy to fool. In *Nature* 574 (7777), pp. 163–166. DOI: 10.1038/d41586-019-03013-5.

Hedewig-Mohr, Sabine (13-Jan-22): Für Marktforscher und Data Scientist: Schweizer Verband lenkt Blick auf fairen Umgang mit Daten. In *horizont*, 13-Jan-22. Available online at https://www.horizont.net/planung-analyse/nachrichten/fuer-marktforscher-und-data-scientist-schweizer-verband-lenkt-blick-auf-fairen-umgang-mit-daten-197074, checked on 09-Aug-22.

Helms, Martine (2004): Food sustainability, food security and the environment. In *British Food Journal* 106 (5), pp. 380–387. DOI: 10.1108/00070700410531606.

Heraclides, Alexis; Dialla, Ada (2016): Humanitarian intervention in the long nineteenth century. Setting the precedent. Manchester, England: Manchester University Press (Humanitarianism : key debates and new approaches Humanitarian intervention in the long nineteenth century. Available online at https://www.manchesteropenhive.com/view/9781526125125/9781526125125.00001.xml. ISBN: 9781526125125.

Hern, Alex (2016): 'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft. In *The Guardian*, 9/28/2016. Available online at https://www.theguardian.com/technology/2016/sep/28/google-facebook-amazon-ibm-microsoft-partnership-on-ai-tech-firms, checked on 4/8/2021.

Hernandez, Frank (2021): The Threat of Social Media to Society and National Security: A Call for Social Media Policy and Legislation. In : a Conference on Culture and Crisis. Available online at https://digitalcommons.liberty.edu/hsgconference/2021/conference_papers/16/.

High, Steven (2002): Deindustrializing Youngstown: Memories of resistance and loss following 'Black Monday', 1977–1997. In : History Workshop Journal: Oxford University Press (54), pp. 100–121. ISBN: 1477-4569. DOI: 10.1093/hwj/54.1.100.

Hill, Kim R.; Walker, Robert S.; Božičević, Miran; Eder, James; Headland, Thomas; Hewlett, Barry et al. (2011): Co-Residence Patterns in Hunter-Gatherer Societies Show Unique Human Social Structure. In *Science (New York, N.Y.)* 331 (6022), pp. 1286–1289. DOI: 10.1126/science.1199071.

Hippisley-Cox, Julia; Pringle, Mike; Cater, Ruth; Wynn, Alison; Hammersley, Vicky; Coupland, Carol et al. (2003): The electronic patient record in primary care—regression or progression? A cross sectional study. In *BMJ (Clinical research ed.)* 326 (7404), pp. 1439–1443. DOI: 1439.

Hitachi (2020): Society 5.0. A people-centric super-smart society / Hitachi-UTokyo Laboratory (H-UTokyo Lab.), editor. Singapore: Springer Open. ISBN: 978-981-15-2988-7.

Hofferbert, Boris (2020): Ist Open Source Software wirklich sicherer? In *heise online*, 9/10/2020. Available online at https://www.heise.de/tipps-tricks/Ist-Open-Source-Software-wirklich-sicherer-3929357.html, checked on 3/16/2021.

Holden, Stein T.; Ghebru, Hosaena (2016): Land tenure reforms, tenure security and food security in poor agrarian economies: Causal linkages and research gaps. In *Global Food Security* 10, pp. 21–28. DOI: 10.1016/j.gfs.2016.07.002.

Holroyd, Carin (2022): Technological innovation and building a 'super smart' society: Japan's vision of society 5.0. In *Journal of Asian Public Policy* 15 (1), pp. 18–31. DOI: 10.1080/17516234.2020.1749340.

Hornik, Kurt (2020): R FAQ. Available online at https://cran.r-project.org/doc/FAQ/R-FAQ.html#What-is-R_003f, updated on 20-Feb-20, checked on 31-May-21.

Horsburgh, Simon; Goldfinch, Shaun; Gauld, Robin (2011): Is Public Trust in Government Associated With Trust in E-Government? In *Social Science Computer Review* 29 (2), pp. 232–241. DOI: 10.1177/0894439310368130.

Human, Soheil; Cech, Florian (2021): A Human-centric Perspective on Digital Consenting: The Case of GAFAM. In : Human Centred Intelligent Systems: Springer, pp. 139–159. DOI: 10.1007/978-981-15-5784-2_12.

ICRC (2010): Cyber warfare. Available online at https://www.icrc.org/en/document/cyber-warfare, checked on 04-Dec-20.

Ioppolo, Giuseppe; Vazquez, Franck; Hennerici, Michael G.; Andrès, Emmanuel (2020): Medicine 4.0: new technologies as tools for a society 5.0: MDPI ,.9) (7). ISBN: 2077-0383.

Ishikawa, Yuki (2002): Calls for deliberative democracy in Japan. In *Rhetoric & Public Affairs* 5 (2), pp. 331–345. DOI: 10.1353/rap.2002.0031.

ISO (2008): Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO/IEC 27000. Available online at https://www.iso.org/standard/73906.html, updated on 08-Oct-20, checked on 08-Oct-20.

ISO (2012): Information technology — Security techniques — Guidelines for cybersecurity. ISO/IEC 27032. Available online at https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en, updated on 22-Sep-20, checked on 22-Sep-20.

ISO (2014): Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO/IEC 27000. Available online at https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-3:en, updated on 22-Sep-20, checked on 22-Sep-20.

Jackman, Joshua A.; Gentile, Douglas A.; Cho, Nam-Joon; Park, Yuhyun (2021): Addressing the digital skills gap for future education. In *Nature Human Behaviour*, pp. 1–4. DOI: 10.1038/s41562-021-01074-z.

Jain, Anshul; Singh, Tanya; Jain, Nitesh (2021): Framework for Securing IoT Ecosystem Using Blockchain: Use Cases Suggesting Theoretical Architecture. In : ICT Systems and Sustainability: Springer, pp. 223–232. DOI: 10.1007/978-981-15-8289-9_21.

Jiang, Min (2010): Authoritarian informationalism: China's approach to Internet sovereignty. In *SAIS Review of International Affairs* 30 (2), pp. 71–89. DOI: 10.1353/sais.2010.0006.

Johnson, L. (2008): Thru the looking glass: Why virtual worlds matter, where they are heading, and why we are all here. In *Address presented at the Federal Consortium on Virtual Worlds, Washington, DC. Retrieved on March* 21.

Kalbalia, Anup (2021): The need for a Certification on Data Structures and Algorithms | LinkedIn. Available online at https://www.linkedin.com/pulse/need-certification-data-structures-algorithms-anup-kalbalia/, updated on 3/16/2021, checked on 3/16/2021.

Karvalics, László Z. (2007): Information Society–what is it exactly?(The meaning, history and conceptual framework of an expression). In *Information Society. From theory to political practice* 29. Available online at http://www.lincompany.kz/pdf/Hungary/02_ZKL_final2007.pdf.

Kaspersky (2020): What is Cyber Security? | Definition, Types, and User Protection | Kaspersky. Available online at https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security, updated on 06-Oct-20, checked on 06-Oct-20.

Kawa, Arkadiusz (2012): SMART Logistics Chain. In Jeng-Shyang Pan, Ngoc Thanh Nguyen, Shiming Chen (Eds.): Intelligent information and database systems. 4th Asian Conference, ACIIDS 2012, Kaohsiung, Taiwan, March 19-21, 2012, Proceedings / Jeng-Shyang Pan, Shyi-Ming Chen, Ngoc Thanh Nguyen, (eds), vol. 7196. Heidelberg: Springer (Lecture notes in artificial intelligence, 0302-9743, 7196-7198), pp. 432–438. ISBN: 978-3-642-28486-1. DOI: 10.1007/978-3-642-28487-8_45.

Kelsey, T. W. (1994): The agrarian myth and policy responses to farm safety. In *American journal of public health* 84 (7), pp. 1171–1177. DOI: 10.2105/ajph.84.7.1171.

Kerzman, Hana; Baron-Epel, Orna; Toren, Orly (2005): What do discharged patients know about their medication? In *Patient education and counseling* 56 (3), pp. 276–282. DOI: 10.1016/j.pec.2004.02.019.

Khare, Anshuman; Odake, Nobutaka; Ishikura, Hiroki (2021): Japanese business operations in an uncertain world. 1st. London: Routledge (Routledge advances in management and business studies. ISBN: 9781003216049.

Kohno, Michinaga; Masuyama, Yoshihiro; Kato, Nobuyuki; Tobe, Akihiko (2011): Hitachi's smart city solutions for new era of urban development. In *Hitachi Review* 60 (2), pp. 79–88. Available online at https://www.hitachi.com/rev/pdf/2011/r2011_02_101.pdf.

Kounavis, Michael; Durham, David; Deutsch, Sergej; Grewal, Ken (2020): Security definitions, entropy measures and constructions for implicitly detecting data corruption. In *Computer Communications* 160, pp. 815–846. DOI: 10.1016/j.comcom.2020.05.022.

Kővári, István; Zimányi, Krisztina (2010): Safety And Security In The Age Of Global Tourism. In *Applied Studies in Agribusiness and Commerce* 4 (5-6), pp. 67–69. DOI: 10.19041/APSTRACT/2010/5-6/11.

Krasner, Stephen D.: The durability of organized hypocrisy. In : Kalmo, Skinner (Ed.) 2010 – Sovereignty in fragments, pp. 96–113. DOI: 10.1017/cbo9780511675928.006.

Krasner, Stephen D. (1999): Sovereignty. Organized hypocrisy. Princeton, N.J.: Princeton University (Princeton paperbacks. Available online at http://www.jstor.org/stable/10.2307/j.ctt7s9d5. ISBN: 069100711X.

Kubin, Emily; Sikorski, Christian von (2021): The role of (social) media in political polarization: a systematic review. In *Annals of the International Communication Association* 45 (3), pp. 188–206. DOI: 10.1080/23808985.2021.1976070.

Kukutai, Tahu; Taylor, John (2016): Indigenous Data Sovereignty. With assistance of Tahu Kukutai, John Taylor: ANU Press. Available online at https://library.oapen.org/handle/20.500.12657/31875.

Kuntsche, Peter; Börchers, Kirstin (2017): Qualitätsmanagement in den gesundheitsversorgenden Sektoren des Gesundheitswesens. In : Qualitäts-und Risikomanagement im Gesundheitswesen: Springer., pp. 289–347. ISBN: 978-3-642-55184-0.

Lange, Christoph; Auer, Sören (2014): Linking Data and Knowledge in Enterprises, Research and Society. In : DB&IS, pp. 3–14. DOI: 10.3233/978-1-61499-458-9-3.

Laudon, Kenneth C.; Laudon, Jane Price (2010): Management information systems: New Jersey: Prentice Hall. ISBN: 978-0-273-78997-0.

Lee, Barbara (1998): Respiratory health hazards in agriculture. In *American journal of respiratory and critical care medicine* 158 (5 Pt 2), S1-S76. DOI: 10.1164/ajrccm.158.supplement_1.rccm1585s1.

Leonard, Mark; Popescu, Nicu; European Council on Foreign Relations (2007): A power audit of EU-Russia relations: European Council on Foreign Relations London. ISBN: 190653800X.

Liao, S. M. (2020): Ethics of artificial intelligence. New York, NY, United States of America: Oxford University Publication. Available online at https://books.google.ch/books?id=1yT3DwAAQBAJ. ISBN: 9780190905057.

Lin, Herbert (2012): Operational considerations in cyber attack and cyber exploitation. In *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*.

Lindner, Martin (2017): Wenn der Hacker Spitalpatienten mitbehandelt. In *Neue Zürcher Zeitung*, 2017. Available online at https://www.nzz.ch/digital/computervirus-wanna-cry-wenn-der-hacker-mitbehandelt-ld.1294555, checked on 12-May-20.

Liu, y.; Qin, H.; Chen, Z.; Shi, C.; Zhang, R.; Chen, W. (2019): Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant. In : 2019

IEEE International Conference on Energy Internet (ICEI), pp. 25–30. DOI: 10.1109/ICEI.2019.00011.

Lomas, William (2009): Conflict, Violence, and Conflict Resolution in Hunting and Gathering Societies. In *The University of Western Ontario Journal of Anthropology* 17 (1). Available online at https://ir.lib.uwo.ca/totem/vol17/iss1/13.

Lu, Hongfang; Huang, Kun; Azimi, Mohammadamin; Guo, Lijun (2019): Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks. In *IEEE Access* 7, pp. 41426–41444. DOI: 10.1109/ACCESS.2019.2907695.

Luft, Gal; Korin, Anne (2009): Energy Security Challenges for the 21st Century. ISBN: 9780275999988.

Luiijf, Eric; Besseling, Kim; Graaf, Patrick de (2013): Nineteen National Cyber Security Strategies. In *International Journal of Critical Infrastructures 6* 9 (1-2), pp. 3–31. DOI: 10.1504/IJCIS.2013.051608.

Lütkepohl, Helmut (2005): New Introduction to Multiple Time Series Analysis. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 9783540277521.

M. Kékes; L. Gábor (2015): Determining the energy supply security of Hungary using the S/D Index. In : 2015 5th International Youth Conference on Energy (IYCE), pp. 1–6. DOI: 10.1109/IYCE.2015.7180778.

Madrigal, Alexis C. (2017): Silicon Valley's Big Three vs. Detroit's Golden-Age Big Three. In *The Atlantic*, 5/24/2017. Available online at https://www.theatlantic.com/technology/archive/2017/05/silicon-valley-big-three/527838/, checked on 3/25/2021.

Manunta, Giovanni (1999): What is Security? In *Security Journal* 12 (3), pp. 57–66. DOI: 10.1057/palgrave.sj.8340030.

Maréchal, Nathalie (2017): Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy. In *Media and Communication* 5 (1), pp. 29–41. DOI: 10.17645/mac.v5i1.808.

Marres, Noortje (2016): Material participation: Technology, the environment and everyday publics: Springer. ISBN: 1137480742.

Massey, Douglas S. (2002): A brief history of human society: The origin and role of emotion in social life. In *American Sociological Review* 67, pp. 1–29. DOI: 10.2307/3088931.

Maurer, Tim (2014): 'Cybersecurity' and Why Definitions Are Risky. Center of Security Studies ETH Zürich. Available online at https://isnblog.ethz.ch/intelligence/cybersecurity-and-the-problem-of-definitions, updated on 02-Dec-20, checked on 02-Dec-20.

Maurice, Pierre; Lavoie, Michel; Laflamme, Lucie; Svanström, Leif; Romer, Claude; Anderson, Ragnar (2001): Safety and Safety Promotion: Definitions for Operational Developments. In *Injury Control and Safety Promotion* 8 (4), pp. 237–240. DOI: 10.1076/icsp.8.4.237.3331.

Mavrodieva, Aleksandrina V.; Shaw, Rajib (2020): Disaster and Climate Change Issues in Japan's Society 5.0—A Discussion. In *Sustainability* 12 (5), p. 1893. DOI: 10.3390/su12051893.

Mcleod, Saul (2007): Maslow's Hierarchy of Needs. Available online at https://www.simplypsychology.org/maslow.html, checked on 4-APR-2022.

McNulty, Brian A.; Jowitt, Simon M. (2021): Barriers to and uncertainties in understanding and quantifying global critical mineral and element supply. In *IScience* 24 (7), p. 102809. DOI: 10.1016/j.isci.2021.102809.

Mees, Heleen (2016): China as the World's Factory. In : The Chinese birdcage: Springer, pp. 21–32. ISBN: 978-1-137-58888-3.

Mehrotra, Abhinav; Bhardwaj, Chhaya (2021): Pegasus has given privacy legislation a jab of urgency. Available online at http://dspace.jgu.edu.in:8080/jspui/handle/10739/4991, checked on 05-Aug-21.

Mehta, Sonam; Bhushan, Bharat; Kumar, Raghvendra (2022): Machine Learning Approaches for Smart City Applications: Emergence, Challenges and Opportunities. In : Recent Advances in Internet of Things and Machine Learning: Springer, Cham, pp. 147–163. Available online at https://link.springer.com/chapter/10.1007/978-3-030-90119-6_12. DOI: 10.1007/978-3-030-90119-6_12.

Merrell, Ian (2022): Blockchain for decentralised rural development and governance. In *Blockchain: Research and Applications*, p. 100086. DOI: 10.1016/j.bcra.2022.100086.

Merriam Webster (2020a): Definition of Cybersecurity. Available online at https://www.merriam-webster.com/dictionary/cybersecurity, updated on 06-Oct-20, checked on 06-Oct-20.

Merriam Webster (2020b): Definition of Security. Available online at https://www.merriam-webster.com/dictionary/security, updated on 22-Sep-20, checked on 22-Sep-20.

Miller, Anthony (2019): The intrinsically linked future for human and Artificial Intelligence interaction. In *Journal of Big Data* 6 (1), pp. 1–9. DOI: 10.1186/s40537-019-0202-7.

Min Jiang (2010): Authoritarian Informationalism: China's Approach to Internet Sovereignty. In *SAIS Review of International Affairs* 30 (2), pp. 71–89. Available online at https://muse.jhu.edu/article/403440.

Mitchell, Gareth (2020): How much data is on the internet? In *BBC Science Focus Magazine*, 2020. Available online at https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/, checked on 12-Oct-20.

Mittelstadt, Brent Daniel; Allo, Patrick; Taddeo, Mariarosaria; Wachter, Sandra; Floridi, Luciano (2016): The ethics of algorithms: Mapping the debate. In *Big Data & Society* 3 (2), 205395171667967. DOI: 10.1177/2053951716679679.

MM Group (2011): Internet world stats-usage and population statistic. Available online at https://www.internetworldstats.com/stats.htm, checked on 5-Mar-22.

Moll, Luis (2002): The Concept of Educational Sovereignty. In *Penn GSE Perspectives on Urban Education* 1 (2), pp. 1–11. Available online at https://urbanedjournal.gse.upenn.edu/.

Mora, Higinio; Mendoza-Tello, Julio C.; Varela-Guzmán, Erick G.; Szymanski, Julian (2021): Blockchain technologies to address smart city and society challenges. In *Computers in Human Behavior* 122, p. 106854. DOI: 10.1016/j.chb.2021.106854.

Moran, Daniel; Russell, James A. (2008): Energy security and global politics: The militarization of resource management: Routledge. ISBN: 1134002009.

Mostaghimi, Bahram (2006): Information Technology and Sovereignty. In *Politics Quarterly* 1(65), pp. 221–251. Available online at https://www.sid.ir/paper/379086/en.

Müller, Klaus (2021): Rede: Algorithmen transparent gestalten - Forderungen an die Politik | VZBV. Available online at https://www.vzbv.de/dokument/rede-algorithmen-transparent-gestalten-forderungen-die-politik, updated on 3/16/2021, checked on 3/16/2021.

Musel, Annabella (2009): Human appropriation of net primary production in the United Kingdom, 1800–2000. In *Ecological Economics* 69 (2), pp. 270–281. DOI: 10.1016/j.ecolecon.2009.08.012.

Nadkarni, Ashwini; Hofmann, Stefan G. (2012): Why do people use Facebook? In *Personality and individual differences* 52 (3), pp. 243–249. DOI: 10.1016/j.paid.2011.11.007.

Nagy, Károly; Hajrizi, Edmond (2019): Building pillars for adapting society 5.0 in post-conflict countries. In *IFAC-PapersOnLine* 52 (25), pp. 40–45. DOI: 10.1016/j.ifacol.2019.12.443.

Narula, Kapil; Reddy, B. Sudhakara (2015): Three blind men and an elephant: The case of energy indices to measure energy security and energy sustainability. In *Energy* 80, pp. 148–158. DOI: 10.1016/j.energy.2014.11.055.

National Academies of Sciences, Engineering, and Medicine (2017): Information technology and the US Workforce: Where are we and where do we go from here?: National Academies Press. ISBN: 0309454026.

National Geographic Society (2019): Hunter-Gatherer Culture. Available online at https://www.nationalgeographic.org/encyclopedia/hunter-gatherer-culture/, updated on 09-Sep-18, checked on 26-Aug-20.

Nature (2018): How one conference embraced diversity. In *Nature* 564 (7735), pp. 161–162. DOI: 10.1038/d41586-018-07718-x.

Nelson, Bradley J.; Dong, Lixin (2010): Nanorobotics. In : Springer handbook of nanotechnology: Springer, pp. 1633–1659. ISBN: 978-3-642-02525-9.

Nelwan, A. F.; Hudaya, C.; Dalimi, R. (2017): Concept development for quantification of integrated energy security. In : 2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering, pp. 394–399. DOI: 10.1109/QIR.2017.8168518.

Nemitz, Paul (2018): Constitutional democracy and technology in the age of artificial intelligence. In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376 (2133). DOI: 10.1098/rsta.2018.0089.

New York state. Legislature. Senate (1841): Documents of the Senate of the State of New York: E. Croswell. Available online at https://books.google.ch/books?id=vfSUgnUMg1MC.

Newborn, Monty (2012): Kasparov versus Deep Blue: Computer chess comes of age: Springer Science & Business Media. ISBN: 1461222605.

Nguyen, Xuan-Thao (2011): The China We Hardly Know: Revealing the New China's Intellectual Property Regime. In *Saint Louis University Law Journal*. Available online at https://hdl.handle.net/1805/5794.

Noble, Safiya Umoja (2018): Algorithms of Oppression. New York: New York University Press. Available online at https://books.google.ch/books?id=g8OSDgAAQBAJ. ISBN: 9781479866762.

Oakes, Charles G. (2009): Safety versus Security in Fire Protection Planning. In *The American Institute of Architects: Knowledge Communities* 85, pp. 43–50. DOI: 10.1016/j.sbspro.2013.08.336.

ODNI (2020): Statement by NCSC Director William Evanina: Election Threat Update for the American Public. The Director of National Intelligence. Available online at https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public, updated on 11/18/2020, checked on 11/18/2020.

OECD (2019a): Artificial Intelligence in Society. Available online at https://www.oecd-ilibrary.org/content/publication/eedfee77-en.

OECD (2019b): Health expenditure in relation to GDP | Health at a Glance 2019 : OECD Indicators | OECD iLibrary. Available online at https://www.oecd-ilibrary.org/sites/592ed0e4-en/index.html?itemId=/content/component/592ed0e4-en, updated on 29-Jun-22, checked on 29-Jun-22.

OECD (2022): Measuring Well-being and Progress: Well-being Research - OECD. Available online at https://www.oecd.org/wise/measuring-well-being-and-progress.htm, updated on 01-Jul-22, checked on 02-Aug-22.

Oehri, Caroline; Teufel, Stephanie (2012): Social Media Security Culture. In : 2012 Information Security for South Africa: IEEE, pp. 1–5. ISBN: 1467321591. DOI: 10.1109/ISSA.2012.6320436.

Ogburn, Monique; Turner, Claude; Dahal, Pushkar (2013): Homomorphic encryption. In *Procedia Computer Science* 20, pp. 502–509. DOI: 10.1016/j.procs.2013.09.310.

Ognibene, Dimitri; Taibi, Davide; Kruschwitz, Udo; Wilkens, Rodrigo Souza; Hernandez-Leo, Davinia; Theophilou, Emily et al. (2021): Challenging Social Media Threats using Collective Well-being Aware Recommendation Algorithms and an Educational Virtual Companion. Available online at https://arxiv.org/pdf/2102.04211.

OHCHR (2022): The human right to adequate housing. Available online at https://www.ohchr.org/en/special-procedures/sr-housing/human-right-adequate-housing, updated on 19-Jul-22, checked on 19-Jul-22.

Okafor, Chigozie Collins; Aigbavboa, Clinton; Thwala, Wellington Didibhuku (2022): A bibliometric evaluation and critical review of the smart city concept – making a case for social equity. In *JSTPM* ahead-of-print (ahead-of-print). DOI: 10.1108/JSTPM-06-2020-0098.

Ong, Homervergel G.; Kim, Young-Dong (2017): The role of wild edible plants in household food security among transitioning hunter-gatherers: evidence from the Philippines. In *Food security* 9 (1), pp. 11–24. DOI: 10.1007/s12571-016-0630-6.

Ortner, Ronald; Leitgeb, Hannes (2011): Mechanizing induction. In : Handbook of the history of logic, vol. 10: Elsevier., pp. 719–772. ISBN: 1874-5857.

Osce, U.s. Mission (2020): United States Condemnation of Russian Cyber-Attack on Georgia. Available online at https://osce.usmission.gov/u-s-condemnation-of-russian-cyber-attack-on-georgia/, updated on 2020, checked on 29-Sep-20.

Osisanya, Segun (2020): National Security versus Global Security | United Nations. UN. Available online at https://www.un.org/en/chronicle/article/national-security-versus-global-security, updated on 4/11/2020, checked on 4/11/2020.

Ouchchy, Leila; Coin, Allen; Dubljević, Veljko (2020): AI in the headlines: the portrayal of the ethical issues of artificial intelligence in the media. In *AI & SOCIETY* 35 (4), pp. 927–936. DOI: 10.1007/s00146-020-00965-5.

Pala, Maria; Olivieri, Anna; Achilli, Alessandro; Accetturo, Matteo; Metspalu, Ene; Reidla, Maere et al. (2012): Mitochondrial DNA signals of late glacial recolonization of Europe from near eastern refugia. In *American journal of human genetics* 90 (5), pp. 915–924. DOI: 10.1016/j.ajhg.2012.04.003.

Paravantis, J. A.; Kontoulis, N.; Ballis, A.; Tsirigotis, D.; Dourmas, V. (2018): A Geopolitical Review of Definitions, Dimensions and Indicators of Energy Security. In : 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), pp. 1–8. DOI: 10.1109/IISA.2018.8633676.

Park, Cyn-Young; Kim, Kijin; Roth, Susann (2020): Global shortage of personal protective equipment amid COVID-19: supply chains, bottlenecks, and policy implications: Asian Development Bank. ISBN: 929262184X.

Paulsson-Holmberg, Tove (1997): Iron Age building offerings: A contribution to the analysis of a die-hard phenomenon in Swedish preindustrial agrarian society. In *Fornvännen* 92 (3/4), pp. 163–175. Available online at http://www.diva-portal.org/smash/get/diva2:1226102/FULLTEXT01.pdf.

Peace, Robin (2001): Social exclusion: A concept in need of definition? In *Social policy journal of New Zealand*, pp. 17–36.

Peltier, Thomas R. (2005): Information security risk analysis: CRC press. ISBN: 0849333466.

Pennsylvania State University (2021): Vector Autoregressive models VAR(p) models. Available online at https://online.stat.psu.edu/stat510/lesson/11/11.2, updated on 31-May-21, checked on 31-May-21.

Peterson, Zachary N. J.; Gondree, Mark; Beverly, Robert (2011): A position paper on data sovereignty: The importance of geolocating data in the cloud. In *In 3rd USENIX Workshop on Hot Topics in Cloud Computing*. DOI: 10.5555/2170444.2170453.

Petrović, Đorđe; Mijailović, Radomir; Pešić, Dalibor (2020): Traffic Accidents with Autonomous Vehicles: Type of Collisions, Manoeuvres and Errors of Conventional Vehicles'

Drivers. In *Transportation Research Procedia* 45, pp. 161–168. DOI: 10.1016/j.trpro.2020.03.003.

Philpott, Daniel (2001): Revolutions in Sovereignty. How Ideas Shaped Modern International Relations. Princeton: Princeton University Press (Princeton studies in international history and politics. ISBN: 9780691057477.

Pichai, Sundar (2018): AI at Google: our principles. In *Google*, 6/7/2018. Available online at https://www.blog.google/technology/ai/ai-principles/, checked on 4/5/2021.

Piirimäe, Pärtel (2011): The Westphalian myth and the idea of external sovereignty. In Hent Kalmo, Quentin Skinner (Eds.): Sovereignty in fragments. The past, present and future of a contested concept. Cambridge: Cambridge University Press, pp. 64–80. ISBN: 9780511675928. DOI: 10.1017/cbo9780511675928.004.

Poblet, Marta; Casanovas, Pompeu; Rodríguez-Doncel, Víctor (2019): Introduction to Linked Data. In : Linked Democracy: Foundations, Tools, and Applications. Cham: Springer International Publishing, pp. 1–25. ISBN: 978-3-030-13363-4. DOI: 10.1007/978-3-030-13363-4_1.

Porter, D. C.; Gujarati, D. N. (2009): Basic econometrics: New York: McGraw-Hill Irwin. ISBN: 978-0-07-233542-2.

Porter, M. E.; Lee, T. H. (2013): The strategy that will fix health care. In *Harvard Business Review* 15. Available online at https://hbr.org/2013/10/the-strategy-that-will-fix-health-care.

Postan, M. M.; Hatcher, John (1978): Agrarian Class Structure and Economic Development in Pre-Industrial Europe. In *Past & Present* 78 (1), pp. 24–37. DOI: 10.1093/past/78.1.24.

Prewett, Kyleen W.; Prescott, Gregory L.; Phillips, Kirk (2020): Blockchain adoption is inevitable—Barriers and risks remain. In *Journal of Corporate accounting & finance* 31 (2), pp. 21–28. DOI: 10.1002/jcaf.22415.

Raaflaub, Christian (2021): Die Maschine und die Moral. Swissinfo. Available online at https://www.swissinfo.ch/ger/kuenstliche-intelligenz_die-maschine-und-die-moral/46186260, updated on 25-Aug-21, checked on 09-Aug-22.

Rahman, Airini Ab; Abdul Hamid, Umar Zakir; Chin, Thoo Ai (2017): Emerging Technologies with Disruptive Effects: A Review. In *PERINTIS eJournal* 7 (2), pp. 111–128. Available online at

https://perintis.org.my/ejournal/wp-content/uploads/2018/11/Paper-4-Vol.-7-No.-2-pp.-111-128.pdf.

Requicha, Aristides AG (2003): Nanorobots, NEMS, and nanoassembly. In *Proceedings of the IEEE* 91 (11), pp. 1922–1933. DOI: 10.1109/JPROC.2003.818333.

Reveron, Derek S.; Savage, John E. (2020): Cybersecurity Convergence: Digital Human and National Security. In *Orbis* 64 (4), pp. 555–570. DOI: 10.1016/j.orbis.2020.08.005.

Risse, Mathias (2019): Human rights and artificial intelligence: An urgently needed agenda. In *Human Rights Quarterly* 41 (1), pp. 1–16. DOI: 10.1353/hrq.2019.0000.

Roberts, Huw; Cowls, Josh; Morley, Jessica; Taddeo, Mariarosaria; Wang, Vincent; Floridi, Luciano (2021): The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. In *AI & SOCIETY* 36 (1), pp. 59–77. DOI: 10.1007/s00146-020-00992-2.

Rojszczak, Marcin (2021): EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses. In *Eur. J. Crime Crim. Law Justice* 29 (3-4), pp. 290–316. DOI: 10.1163/15718174-bja10027.

Rona, Gabor; Aarons, Lauren (2015): State responsibility to respect, protect and fulfill human rights obligations in cyberspace. In *J. Nat'l Sec. L. & Pol'y* 8, pp. 503–530. Available online at https://jnslp.com/wp-content/uploads/2017/10/State-Responsibility-to-Respect_2.pdf.

Rosegrant, Mark W.; Cline, Sarah A. (2003): Global food security: challenges and policies. In *Science* 302 (5652), pp. 1917–1919. DOI: 10.1126/science.1092958.

Rotman, David (2013): How Technology Is Destroying Jobs. In *MIT Technology Review*, 6/12/2013. Available online at https://www.technologyreview.com/2013/06/12/178008/how-technology-is-destroying-jobs/, checked on 2/16/2021.

Rowe, Gene; Frewer, Lynn J. (2005): A typology of public engagement mechanisms. In *Science, Technology, & Human Values* 30 (2), pp. 251–290. DOI: 10.1177/0162243904271724.

Rozanova, Nadezhda M. (2021): Competition and monopoly in a digital era. In *Obshchestvennye nauki i sovremennost* (1), pp. 63–72. DOI: 10.31857/S086904990014000-2.

Rumberger, Russell W. (1984): High technology and job loss. In *Technology in Society* 6 (4), pp. 263–284. DOI: 10.1016/0160-791X(84)90022-8.

Runciman, William; Hibbert, Peter; Thomson, Richard; van der Schaaf, Tjerk; Sherman, Heather; Lewalle, Pierre (2009): Towards an International Classification for Patient Safety: key concepts and terms. In *International journal for quality in health care* 21 (1), pp. 18–26. DOI: 10.1093/intqhc/mzn057.

Russell, Stuart (2019): Human compatible: Artificial intelligence and the problem of control: Penguin. ISBN: 0525558624.

Saldivar, Jorge; Parra, Cristhian; Laconich, Mical; Cernuzzi, Luca (2022): The electoral success of social media losers: a study on the usage and influence of Twitter in times of elections in Paraguay. In *SN Social Sciences* 2 (7), pp. 1–31. DOI: 10.1007/s43545-022-00392-x.

Salgues, Bruno (2018): Society 5.0: industry of the future, technologies, methods and tools: John Wiley & Sons. ISBN: 1119527619.

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017): Towards a more representative definition of cyber security. In *Journal of Digital Forensics, Security and Law* 12 (2), pp. 53–74. DOI: 10.15394/jdfsl.2017.1476.

Scheibmeir, Jim A.; Malaiya, Yashwant K. (2021): Social media analytics of the Internet of Things. In *Discover Internet of Things* 1 (1), pp. 1–15. DOI: 10.1007/s43926-021-00016-5.

Schless, Hank (2022): Protect Yourself from Powerful Pegasus Spyware. Available online at https://www.lookout.com/blog/protect-against-pegasus-spyware, updated on 09-Aug-22, checked on 09-Aug-22.

Schlienger, Thomas; Teufel, Stephanie (2002): Information security culture. In : Security in the Information Society: Springer, pp. 191–201. DOI: 10.1007/978-0-387-35586-3_46.

Schlienger, Thomas; Teufel, Stephanie (2003): Information security culture-from analysis to change. In *South African Computer Journal* 2003 (31), pp. 46–52. Available online at https://hdl.handle.net/10520/EJC27949.

Schmandt, Jurgen; Wilson, Robert; Smith, Suzanne E.; Muller, Brian H. (2019): Promoting high technology industry: Initiatives and policies for state governments: Routledge. ISBN: 1000308340.

Schmidhuber, Josef; Tubiello, Francesco N. (2007): Global food security under climate change. In *Proceedings of the National Academy of Sciences of the United States of America* 104 (50), pp. 19703–19708. DOI: 10.1073/pnas.0701976104.

Schmidt, Jan-Simon; Osebold, Rainard (2017): Environmental management systems as a driver for sustainability. state of implementation, benefits and barriers in German construction companies. In *Journal of Civil Engineering and Management* 23 (1), pp. 150–162. DOI: 10.3846/13923730.2014.946441.

Schwab, Klaus (2016): The Fourth Industrial Revolution. Geneva, Switzerland: World Economic Forum. ISBN: 1524758876.

Scutti, S. (2017): 'automated dermatologist'detects skin cancer with expert accuracy. In *CNN (https://edition. cnn. com/2017/01/26/health/ai-system-detects-skincancer-study/index. html)*.

Sevilla Guzmán, Eduardo; Woodgate, Graham (2013): Agroecology: Foundations in Agrarian Social Thought and Sociological Theory. In *Agroecology and Sustainable Food Systems* 37 (1), pp. 32–44. DOI: 10.1080/10440046.2012.695763.

Shah, M. M. (2008): Sustainable Development. In Sven Erik Jorgensen (Ed.): Encyclopedia of ecology. Amsterdam: Elsevier, pp. 3443–3446. ISBN: 9780080454054. DOI: 10.1016/B978-008045405-4.00633-9.

Shiroishi, Yoshihiro; Uchiyama, Kunio; Suzuki, Norihiro (2018): Society 5.0: For Human Security and Well-Being. In *Computer* 51 (7), pp. 91–95. DOI: 10.1109/MC.2018.3011041.

Sierra, Dannelle P.; Weir, Nathan A.; Jones, James Frank (2005): A review of research in the field of nanorobotics. In *A review of research in the field of nanorobotics*. DOI: 10.2172/875622.

Silver, Hilary (2007): The process of social exclusion: the dynamics of an evolving concept. In *Chronic Poverty Research Centre Working Paper* (95). Available online at https://www.chronicpoverty.org/pubfiles/95Silver.pdf.

Sima, Violeta; Gheorghe, Ileana Georgiana; Subić, Jonel; Nancu, Dumitru (2020): Influences of the industry 4.0 revolution on the human capital development and consumer behavior: A systematic review. In *Sustainability* 12 (10), p. 4035. DOI: 10.3390/su12104035.

Simonofski, Anthony; Asensio, Estefanía Serral; Wautelet, Yves (2019): Citizen participation in the design of smart cities: Methods and management framework. In : Smart cities: Issues and challenges: Elsevier, pp. 47–62. DOI: 10.1016/B978-0-12-816639-0.00004-1.

Slonje, Robert; Smith, Peter K. (2008): Cyberbullying: Another main type of bullying? In *Scandinavian journal of psychology* 49 (2), pp. 147–154. DOI: 10.1111/j.1467-9450.2007.00611.x.

Smith, Clifton L.; Brooks, David J. (2013): Security science. The theory and practice of security. Online-ausg. Amsterdam: Elsevier, BH. Available online at http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=485991&site=ehost-live. ISBN: 9780123944368.

Smutny, Pavel; Schreiberova, Petra (2020): Chatbots for learning: A review of educational chatbots for the Facebook Messenger. In *Computers & Education* 151, p. 103862. DOI: 10.1016/j.compedu.2020.103862.

Sørensen, Lasse; Karg, Sabine (2014): The expansion of agrarian societies towards the north – new evidence for agriculture during the Mesolithic/Neolithic transition in Southern Scandinavia. In *Journal of Archaeological Science* 51, pp. 98–114. DOI: 10.1016/j.jas.2012.08.042.

Spanjer, Aldo (2007): Russian gas price reform and the EU–Russia gas relationship: Incentives, consequences and European security of supply. In *Energy policy* 35 (5), pp. 2889–2898. DOI: 10.1016/j.enpol.2006.10.019.

Spatz, Erica S.; Elwyn, Glyn; Moulton, Benjamin W.; Volk, Robert J.; Frosch, Dominick L. (2017): Shared decision making as part of value based care: new US policies challenge our readiness. In *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen* 123, pp. 104–108. DOI: 10.1016/j.zefq.2017.05.012.

Spycher, Jannick (2021): Switzerland 5.0 Forecast of a future super smart society with an overlook on opportunities and challenges. Master Thesis. University of Fribourg. iimt.

Sreelakshmi, K. K.; Bhatia, Ashutosh; Agrawal, Ankit (2021): Securing IoT Applications Using Blockchain. In *Blockchain Applications in IoT Security*, pp. 56–83. DOI: 10.4018/978-1-7998-2414-5.ch004.

Stanton, Jeffrey M. (2001): Galton, Pearson, and the Peas: A Brief History of Linear Regression for Statistics Instructors. In *Journal of Statistics Education* 9 (3). DOI: 10.1080/10691898.2001.11910537.

Su, Grace (2018): Unemployment in the AI Age. In *AI Matters* 3 (4), pp. 35–43. DOI: 10.1145/3175502.3175511.

Suissa, Amnon Jacob (2015): Cyber addictions: toward a psychosocial perspective. In *Addictive Behaviors* 43, pp. 28–32. DOI: 10.1016/j.addbeh.2014.09.020.

Summers, G.; Koehne, H. (2004): Data and databases. In *Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5*.

Takahashi, Taiki (2018): Behavioral Economics of Addiction in the Age of a Super Smart Society: Society 5.0. In *Oukan* 12 (2), pp. 119–122. DOI: 10.11487/trafst.12.2_119.

Tankard, Colin (2012): Big data security. In *Network security* 2012 (7), pp. 5–8. DOI: 10.1016/S1353-4858(12)70063-6.

Tanrikulu, Ibrahim; Erdur-Baker, Özgür (2021): Psychometric properties of a Cyberbullying Inventory for university students. In *British Journal of Guidance & Counselling* 49 (3), pp. 494–507. DOI: 10.1080/03069885.2020.1775174.

Teufel, Bernd; Sentic, Anton (2022): Blockchain in Energy. In *The 4Ds of Energy Transition: Decarbonization, Decentralization, Decreasing Use and Digitalization*, pp. 381–397. DOI: 10.1002/9783527831425.ch18.

Teufel, Bernd; Sentic, Anton; Barmet, Mathias (2019): Blockchain energy: Blockchain in future energy systems. In *Journal of Electronic Science and Technology* 17 (4), p. 100011. DOI: 10.1016/j.jnlest.2020.100011.

Teufel, Stephanie; Teufel, Bernd (2014): The Crowd Energy Concept. In *Journal of Electronic Science and Technology* 12 (3), pp. 263–269. DOI: 10.3969/j.issn.1674-862X.2014.03.006.

Teufel, Stephanie; Teufel, Bernd (2015): Crowd Energy Information Security Culture - Security Guidelines for Smart Environments. In : 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity). 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), pp. 123–128. DOI: 10.1109/SmartCity.2015.58.

Teufel, Stephanie; Teufel, Bernd (Eds.) (2019): The Positive Momentum of Crowds for the Implementation of Smart Environments. International Conference on Social Sciences and Management (ICSSM). Beijing, June. pp 78-88. Available online at http://aceai.org/data/file/20190619/20190619183009_30207.pdf.

Teufel, Stephanie; Teufel, Bernd; Aldabbas, Mohammad; Nguyen, Minh (2020): Cyber Security Canvas for SMEs. In Hein Venter, Marianne Loock, Marijke Coetzee, Mariki Eloff, Jan Eloff, Reinhardt Botha (Eds.): Information and Cyber Security, vol. 1339. Cham: Springer, Cham (Communications in Computer and Information Science), pp. 20–33. ISBN: 978-3-030-66038-3. DOI: 10.1007/978-3-030-66039-0_2.

Thornton, Sarah M.; Pan, Selina; Erlien, Stephen M.; Gerdes, J. Christian (2017): Incorporating Ethical Considerations Into Automated Vehicle Control. In *IEEE Trans. Intell. Transport. Syst.* 18 (6), pp. 1429–1439. DOI: 10.1109/tits.2016.2609339.

Tran, Quang Thanh; Hao, Li; Trinh, Quang Khai (2020): A comprehensive research on exponential smoothing methods in modeling and forecasting cellular traffic. In *Concurrency Computat Pract Exper* 32 (23). DOI: 10.1002/cpe.5602.

Trenca, Ioan; Mutu, Simona; Dezsi, Eva (2011): Advantages and limitations of VAR models used in managing market risk in banks. In *Finance–Challenges of the Future* 13, pp. 32–43. Available online at https://feaa.ucv.ro/FPV/013-05.pdf.

Tuck, R. (2001): The Rights of War and Peace: Political Thought and the International Order from Grotius to Kant: OUP Oxford. Available online at https://books.google.ch/books?id=BXNYAwAAQBAJ. ISBN: 9780191037429.

Tufekci, Zeynep (2017): We're building a dystopia just to make people click on ads. Available online at https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads?language=en, updated on 11-May-20, checked on 11-May-20.

Turchet, Luca; Chan, Nam Ngo (2022): Blockchain-based Internet of Musical Things. In *Blockchain: Research and Applications* 3 (3), p. 100083. DOI: 10.1016/j.bcra.2022.100083.

Tushingham, Shannon; Bettinger, Robert L. (2019): Storage defense: Expansive and intensive territorialism in hunter-gatherer delayed return economies. In *Quaternary International* 518, pp. 21–30. DOI: 10.1016/j.quaint.2018.02.013.

U.S. Copyrights Office (2021): Fair Use (FAQ) | U.S. Copyright Office. Available online at https://www.copyright.gov/help/faq/faq-fairuse.html, updated on 1/25/2021, checked on 3/15/2021.

UNESCO (2017): Nation-State | United Nations Educational, Scientific and Cultural Organization. Available online at https://wayback.archive-it.org/10611/20171126022449/http://www.unesco.org/new/en/social-and-human-sciences/themes/international-migration/glossary/nation-state/, updated on 3/12/2021, checked on 3/12/2021.

UNIL (2019): Data life cycle & types. Edited by UNIL Open Science. University of Lausanne. Available online at https://www.unil.ch/openscience/en/home/menuinst/open-research-data/les-donnees-de-recherche/cycle-de-vie-et-types-de-donnees.html, updated on 19-Aug-20, checked on 13-Oct-20.

United Nations (2005): 2005 World Summit Outcome. Available online at https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf.

United Nations (2006): The "Kronprins Gustaf Adolf" (Sweden, USA). Available online at https://legal.un.org/riaa/cases/vol_II/1239-1305.pdf, checked on 2/26/2021.

United Nations (2010): 'Our Challenges Are Shared; So, Too, Is Our Commitment to Enhance Freedom from Fear, Freedom from Want, Freedom to Live in Dignity', Says Secretary-General. Available online at https://www.un.org/press/en/2010/ga10942.doc.htm, updated on 9/11/2020, checked on 9/11/2020.

United Nations (2019): The age of digital interdependence, Report of the UN Secretary General's High-Level Panel on Digital Cooperation: Geneva: Un Secretary General.

United Nations (2020): Take Action for the Sustainable Development Goals. Available online at https://www.un.org/sustainabledevelopment/sustainable-development-goals/, updated on 29-Sep-20, checked on 29-Sep-20.

US Department of Health and Human Services (1999): Mental health: A report of the Surgeon General: US Department of Health and Human Services, Substance Abuse. Available online at https://profiles.nlm.nih.gov/spotlight/nn/catalog/nlm:nlmuid-101584932X120-doc.

Valeggia, Claudia; Ellison, Peter T. (2004): Lactational amenorrhoea in well-nourished Toba women of Formosa, Argentina. In *Journal of biosocial science* 36 (5), pp. 573–595. DOI: 10.1017/s0021932003006382.

Vardi, Moshe Y. (2015): Is information technology destroying the middle class? In *Communications of the ACM* 58 (2), p. 5. DOI: 10.1145/2666241.

Vasauskaite, Jovita; Teufel, Stephanie; Teufel, Bernd (2017): Smart Framework: Application under the Conditions of Modern Economy. In *EE* 28 (2). DOI: 10.5755/j01.ee.28.2.17631.

Veney, James E.; Luckey, James W. (1983): A comparison of regression and ARIMA models for assessing program effects: An application to the mandated highway speed limit reduction of 1974. In *Social Indicators Research* 12 (1), pp. 83–105. Available online at https://www.jstor.org/stable/27521083.

Vincent, James (2021): OpenAI's state-of-the-art machine vision AI is fooled by handwritten notes. In *The Verge*, 3/8/2021. Available online at https://www.theverge.com/2021/3/8/22319173/openai-machine-vision-adversarial-typographic-attacka-clip-multimodal-neuron, checked on 3/29/2021.

Vivoda, Vlado (2010): Evaluating energy security in the Asia-Pacific region: A novel methodological approach. In *Energy policy* 38 (9), pp. 5258–5263. DOI: 10.1016/j.enpol.2010.05.028.

von Solms, Rossouw (1998): Information security management (3): the code of practice for information security management (BS 7799). In *Info Mngmnt & Comp Security*. DOI: 10.1108/09685229810240158.

von Solms, Rossouw; van Niekerk, Johan (2013): From information security to cyber security. In *Computers & Security* 38, pp. 97–102. DOI: 10.1016/j.cose.2013.04.004.

WÆver, Ole (2008): The Changing Agenda of Societal Security. In Hans Günter Brauch (Ed.): Globalization and environmental challenges, vol. 3. Berlin: Springer (Hexagon series on

human and environmental security and peace, 1865-5793, v. 3), pp. 581–593. ISBN: 978-3-540-75976-8. DOI: 10.1007/978-3-540-75977-5_44.

WÆver, Ole; Carlton, David (1993): Identity, migration and the new security agenda in Europe. London: Pinter. ISBN: 1855670410.

Walker, Robert S.; Hill, Kim R.; Flinn, Mark V.; Ellsworth, Ryan M. (2011): Evolutionary history of hunter-gatherer marriage practices. In *PloS one* 6 (4), e19066. DOI: 10.1371/journal.pone.0019066.

Walls, A.; Perkins, E.; Weiss, J. (2013): Definition: Cybersecurity. In *Retrieved from Gartner. com website: https://www. gartner. com/doc/2510116/def inition-cybersecurity*.

Wang, Xiao; Li, Lingxi; Yuan, Yong; Ye, Peijun; Wang, Fei-Yue (2016): ACP-based social computing and parallel intelligence: Societies 5.0 and beyond. In *CAAI Transactions on Intelligence Technology* 1 (4), pp. 377–393. DOI: 10.1016/j.trit.2016.11.005.

Warkentin, Merrill; Willison, Robert (2009): Behavioral and policy issues in information systems security: the insider threat. In *European Journal of Information Systems* 18 (2), pp. 101–105. DOI: 10.1057/ejis.2009.12.

Weng, Yueh-Hsuan; Chen, Chien-Hsun; Sun, Chuen-Tsai (2009): Toward the human–robot co-existence society:on safety intelligence for next generation robots. In *Int J of Soc Robotics* 1 (4), pp. 267–282. DOI: 10.1007/s12369-009-0019-1.

Wheeler, Amanda; Scahill, Shane; Hopcroft, David; Stapleton, Helen (2018): Reducing medication errors at transitions of care is everyone's business. In *Australian Prescriber* 41 (3), p. 73. DOI: 10.18773/austprescr.2018.021.

Wheeler, Tim; Braun, Joachim von (2013): Climate change impacts on global food security. In *Science* 341 (6145), pp. 508–513. DOI: 10.1126/science.1239402.

Whitehouse, Nicki J.; Kirleis, Wiebke (2014): The world reshaped: practices and impacts of early agrarian societies. Journal of Archaeological Science, 51, 1-11. In *Journal of Archaeological Science* 51, pp. 1–11. DOI: 10.1016/J.JAS.2014.08.007.

Whitman, M. E.; Mattord, H. J. (2009): Principles of Information Security (4e). ISBN: 978-1-111-13821-9.

Winfield, Alan F. T.; Jirotka, Marina (2018): Ethical governance is essential to building trust in robotics and artificial intelligence systems. In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376 (2133), p. 20180085. DOI: 10.1098/rsta.2018.0085.

Wing, Jeannette M. (2019): The Data Life Cycle. In *Harvard Data Science Review* 1 (1). DOI: 10.1162/99608f92.e26845b4.

Winick, Erin (25-Jan-18): Every study we could find on what automation will do to jobs, in one chart. In *MIT Technology Review*, 25-Jan-18. Available online at https://www.technologyreview.com/2018/01/25/146020/every-study-we-could-find-on-what-automation-will-do-to-jobs-in-one-chart/, checked on 28-Jul-22.

Wolfers, Arnold (1952): " National security" as an ambiguous symbol. In *Political science quarterly* 67 (4), pp. 481–502. DOI: 10.2307/2145138.

World Bank (2019): Individuals using the Internet (% of population) | Data. Available online at https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2019&start=1990, updated on 19-Jul-22, checked on 19-Jul-22.

World Bank (2021a): Glossary | DataBank. Available online at https://databank.worldbank.org/metadataglossary/jobs/series/NY.GDP.MKTP.KD.ZG, updated on 26-May-21, checked on 26-May-21.

World Bank (2021b): Glossary | DataBank. Available online at https://databank.worldbank.org/metadataglossary/health-nutrition-and-population-statistics/series/NY.GNP.PCAP.CD, updated on 26-May-21, checked on 26-May-21.

World Bank (2021c): Switzerland | Data. Available online at https://data.worldbank.org/country/switzerland, updated on 06-May-21, checked on 06-May-21.

World Economic Forum (2019): Modern society has reached its limits. Society 5.0 will liberate us. Available online at https://www.weforum.org/agenda/2019/01/modern-society-has-reached-its-limits-society-5-0-will-liberate-us/, updated on 22-Jun-21, checked on 22-Jun-21.

World Economic Forum (2020): The Global Competitiveness Report. Special Edition 2020. 2020 ed. Cologny/Geneva: World Economic Forum (The global competitiveness report /

World Economic Forum,.Special edition 2020). Available online at https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2020.pdf, checked on 20-Jul-22. ISBN: 9782940631179.

World Economic Forum (2021): Top 9 ethical issues in artificial intelligence. Available online at https://www.weforum.org/agenda/2016/10/top-10-ethical-issues-in-artificial-intelligence/, updated on 3/19/2021, checked on 3/19/2021.

Wu, Timothy S. (1997): Cyberspace Sovereignty--The Internet and the International System. In *Harv. JL & Tech.* 10, p. 647. Available online at http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech647.pdf.

Yong, Ed (2018): A Popular Algorithm Is No Better at Predicting Crimes Than Random People. In *The Atlantic*, 1/29/2018. Available online at https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/, checked on 3/19/2021.

Young, Kimberly S. (1998): Internet Addiction: The Emergence of a New Clinical Disorder. In *Cyberpsychology & behavior* 1 (3), pp. 237–244. DOI: 10.1089/cpb.1998.1.237.

Young, William; Leveson, Nancy (2013): Systems thinking for safety and security. In : Proceedings of the 29th Annual Computer Security Applications Conference, pp. 1–8.

Zabel, Christine (2018): Challenges of Food Security: Free Trade, Distribution and Political (In)Stability in Mid 18th Century France. In *Eur J Secur Res* 3 (1), pp. 35–50. DOI: 10.1007/s41125-017-0023-7.

Zhenmin, Liu (2020): Recover better: Economic and social challenges and opportunities - World. Edited by United Nations [UN] – Department of Economic and Social Affairs (DESA). Available online at https://www.un.org/development/desa/en/wp-content/uploads/2020/07/RECOVER_BETTER_0722-1.pdf, updated on 22-Jun-21, checked on 22-Jun-21.

Zhou, Chuanlong; Zhu, Biqing; Davis, Steven J.; Liu, Zhu; Halff, Antoine; Arous, Simon Ben et al. (2022): Natural gas supply from Russia derived from daily pipeline flow data and potential solutions for filling a shortage of Russian supply in the European Union (EU). In *Earth System Science Data Discussions*, pp. 1–19. DOI: 10.5194/essd-2022-246.

Zhu, Guiyang; Chou, Mabel C.; Tsai, Christina W. (2020): Lessons learned from the COVID-19 pandemic exposing the shortcomings of current supply chain operations: a long-term prescriptive offering. In *Sustainability* 12 (14), p. 5858. DOI: 10.22617/BRF200128-2.

Zhu, Lei; Zheng, Qianwen (2020): The impact of the Social Security Fund on auditor litigation risk. In *China Journal of Accounting Research* 13 (2), pp. 201–221. DOI: 10.1016/j.cjar.2020.05.002.

7 Appendix

All the dissertation's supplemental data, analysis, and sources are included in the appendices.

7.1 Sample Interview Questions

The complete interview transcript is available in (Spycher 2021). This part provides some of the questions asked to the interview partners. The aim is to give the reader an idea of the nature of the questions. Hence, the interview's language is German.

Wo werden uns Technologien wie AI, Big Data, Blockchain usw. hinbringen? Wie wird sich die Gesellschaft dadurch verändern?
Welche Auswirkungen hat die Digitalisierung auf unsere zukünftigen Jobs, die Bildung, das Gesundheitsweisen (bspw. EPD), Mobilität/Transportwesen, Tele-working (momentan häufig auch gezwungenermassen durch COVID-19 / Wo liegen hier aber die Chancen nach COVID-19? / Werden wir in Zukunft ganz anders arbeiten?)
Fachkräftemangel: Was sollte sich in der Bildung in Zukunft ändern?
Digitaler wilder Westen: Tut der Staat genug um uns (und bspw. Unsere Daten) vor künftigen Gefahren zu schützen? Sollte sich der Staat hier überhaupt einmischen?
Haben gewisse Technologien negative Folgen? Sollten deshalb gewisse Technologien durch den Staat reguliert oder gar verboten werden? Wie würde sich das auf die Wettbewerbsposition der Schweiz auswirken?
Digitale Ethik: Wie schaffen wir es in der Schweiz eine ethisch vertretbare Digitalisierung zu gewährleisten? Wer sollte hier regulieren?
Wo werden uns Technologien wie AI, Big Data, Blockchain usw. hinbringen? Wie wird sich die Gesellschaft dadurch verändern?
Haben gewisse Technologien negative Folgen? Sollten deshalb gewisse Technologien durch den Staat reguliert oder gar verboten werden? Wie würde sich das auf die Wettbewerbsposition der Schweiz auswirken?

7.2 Forecasting and Modelling All Variables

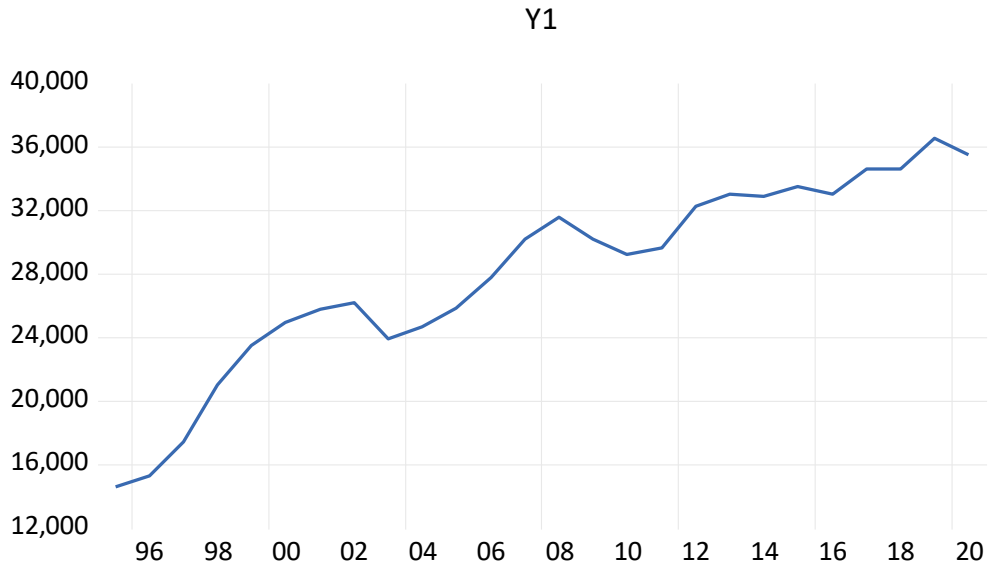
This section forecasts and models all variables using ARIMA Models and Exponential Smoothing ETS.

7.2.1 Modeling ICT investments y1

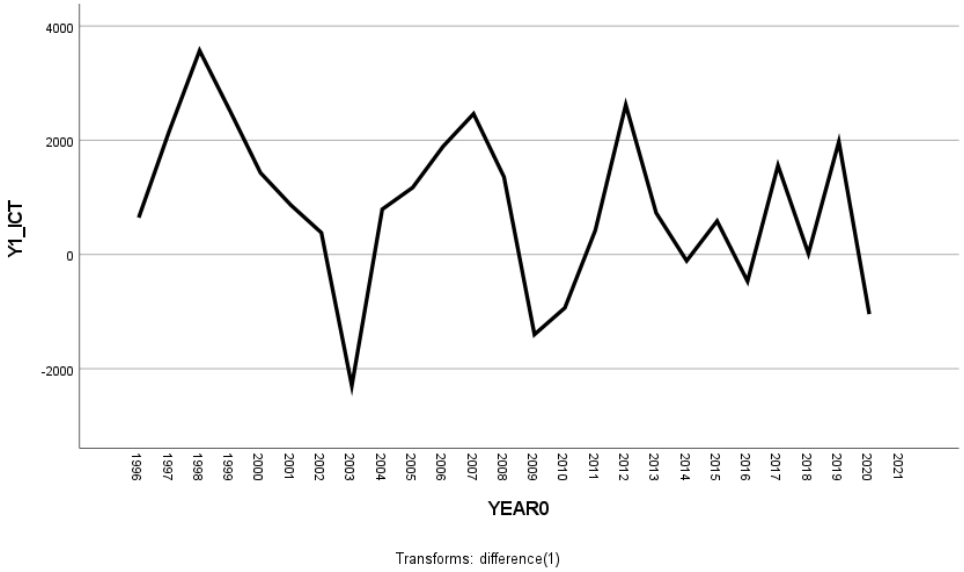
Modeling and forecasting ICT using the historic values from 1995 through 2020. The data is published by the FSO.

Year	ICT	Year	ICT	Year	ICT
1995	14,598	2004	24,658	2013	32,987
1996	15,244	2005	25,831	2014	32,877
1997	17,402	2006	27,725	2015	33,463
1998	20,972	2007	30,189	2016	32,995
1999	23,486	2008	31,547	2017	34,554
2000	24,917	2009	30,147	2018	34,572
2001	25,782	2010	29,214	2019	36,547
2002	26,164	2011	29,639	2020	35,504
2003	23,866	2012	32,260		

The first step is to determine the stationarity of the series by using the Dick-Fuller test.



The plot shows that the series is non-stationary. It has a linear increasing trend overtime. Therefore, the first differencing is taken as shown in the plot



It is obvious visually that the series is stationary after taking the first difference which is enough proof. Nevertheless, the unit root (Dicky-Fuller) test is made using EViews software.

Null Hypothesis: Y1 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.270382	0.1886
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

P value = 0.18 > 0.05 this implies that Y1 is nonstationary as we cannot reject the null hypothesis H0. Therefore, Y1 has a unit root.

Additionally, the absolute value of the t-test is smaller than the t-value at 0.05. which indicates the same outcome: Y1 is nonstationary.

The same test is made again but this time by taking the first order difference.

Null Hypothesis: D(Y1) has a unit root
Exogenous: Constant
Lag Length: 2 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.216958	0.0037
Test critical values:	1% level	-3.769597	
	5% level	-3.004861	
	10% level	-2.642242	

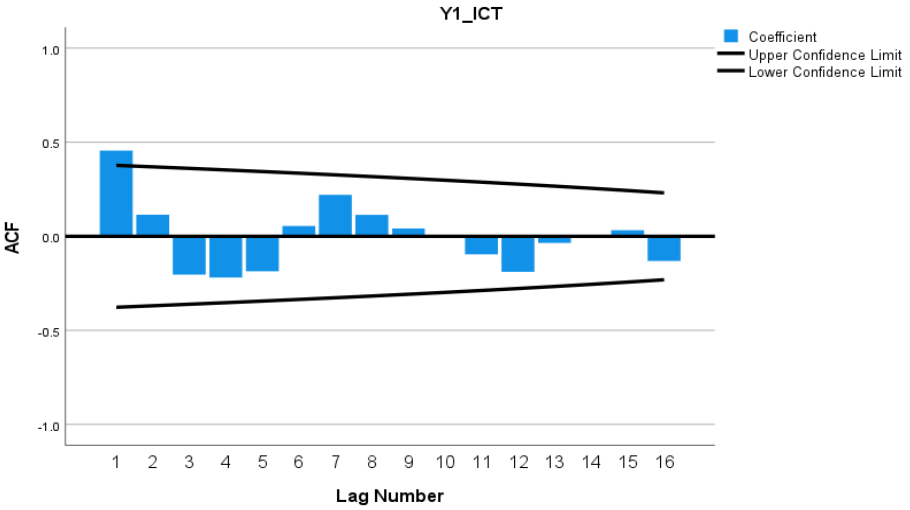
*MacKinnon (1996) one-sided p-values.

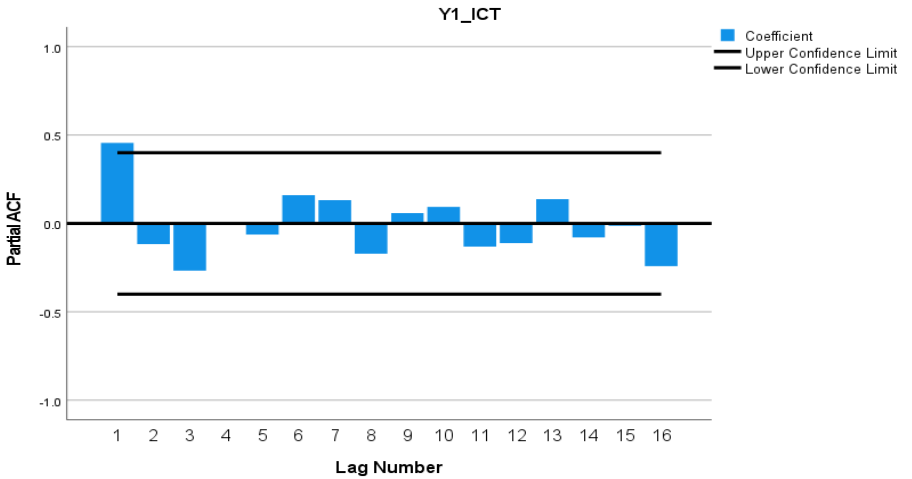
P value = 0.003 < 0.05

We reject the H0. Y1 is stationary after taking the first order difference. This mean that the ARIMA model parameter D=1.

Likewise, the absolute value of the t-test is greater than the t-value at 0.05 which means Y1 is stationary after taking the first order difference.

The correlogram of the autocorrelation function and partial autocorrelation function is necessary to determine the other two ARIMA parameters. Hence, the natural logarithm transformation of the series with the proper differencing has to be taken. Otherwise, the correlogram will carry no significance.





The figures show that both ACF and PACF have a cut-off after the first lag. The considered values for the parameters p, q are 1,1. However the zero value should also be in consideration. The potential ARIMA models are ARIMA (1,1,1), ARIMA (0,1,1), and ARIMA (1,1,0)

ARIMA (1,1,1) is not a good model because p values for the coefficients of the AR and MA are higher than 0.05

Dependent Variable: D(NLY1)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/07/22 Time: 16:18
Sample: 1996 2020
Included observations: 25
Failure to improve objective (non-zero gradients) after 36 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.035272	0.027673	1.274624	0.2164
AR(1)	0.965455	0.770403	1.253181	0.2239
MA(1)	-1.000000	4304.485	-0.000232	0.9998
SIGMASQ	0.003275	0.339330	0.009650	0.9924

R-squared	0.021997	Mean dependent var	0.035550
Adjusted R-squared	-0.117717	S.D. dependent var	0.059058
S.E. of regression	0.062437	Akaike info criterion	-2.549094
Sum squared resid	0.081867	Schwarz criterion	-2.354074
Log likelihood	35.86368	Hannan-Quinn criter.	-2.495004
F-statistic	0.157444	Durbin-Watson stat	1.026516
Prob(F-statistic)	0.923701		

Inverted AR Roots	.97
Inverted MA Roots	1.00

ARIMA (1,1,0) is a good model for fitting the series.

Dependent Variable: D(NLY1)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/07/22 Time: 16:21
Sample: 1996 2020
Included observations: 25
Convergence achieved after 9 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.033730	0.019419	1.737008	0.0964
AR(1)	0.461396	0.215045	2.145572	0.0432
SIGMASQ	0.002616	0.000837	3.126471	0.0049

R-squared	0.218784	Mean dependent var	0.035550
Adjusted R-squared	0.147765	S.D. dependent var	0.059058
S.E. of regression	0.054520	Akaike info criterion	-2.858749
Sum squared resid	0.065394	Schwarz criterion	-2.712484
Log likelihood	38.73437	Hannan-Quinn criter.	-2.818182
F-statistic	3.080622	Durbin-Watson stat	1.752358
Prob(F-statistic)	0.066142		

Inverted AR Roots	.46

ARIMA (0,1,1) is not a good fit because the p value of MA coefficient is bigger than 0.05.

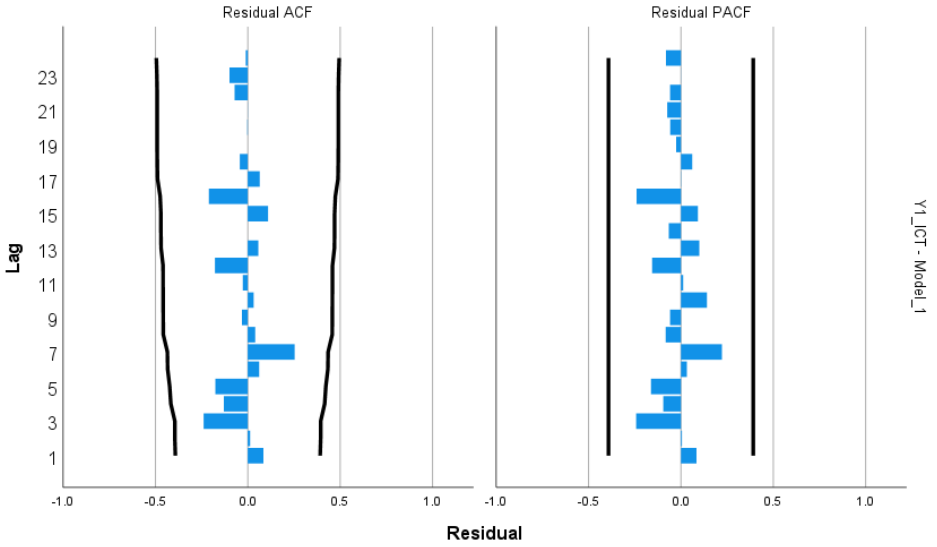
Dependent Variable: D(NLY1)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/07/22 Time: 16:22
Sample: 1996 2020
Included observations: 25
Convergence achieved after 35 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.034101	0.015714	2.170141	0.0411
MA(1)	0.405529	0.228402	1.775504	0.0897
SIGMASQ	0.002701	0.000844	3.202495	0.0041

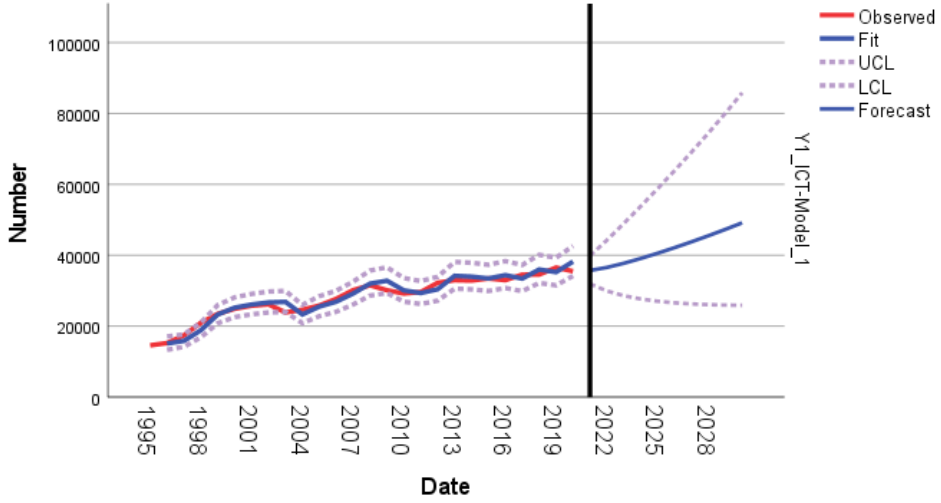
R-squared	0.193190	Mean dependent var	0.035550
Adjusted R-squared	0.119844	S.D. dependent var	0.059058
S.E. of regression	0.055406	Akaike info criterion	-2.828901
Sum squared resid	0.067536	Schwarz criterion	-2.682636
Log likelihood	38.36126	Hannan-Quinn criter.	-2.788333
F-statistic	2.633945	Durbin-Watson stat	1.684629
Prob(F-statistic)	0.094294		

Inverted MA Roots	-.41

The analysis of the residuals shows only white noise. No value has statistical significance.



The forecasted values and the fitted model are presented. The graph shows that the model is a good fit to the observed data.

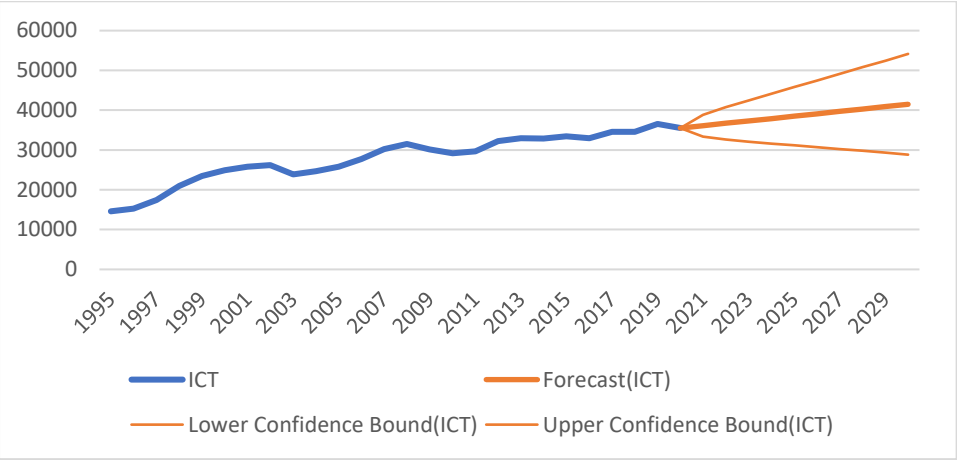


the parameters of the model are below

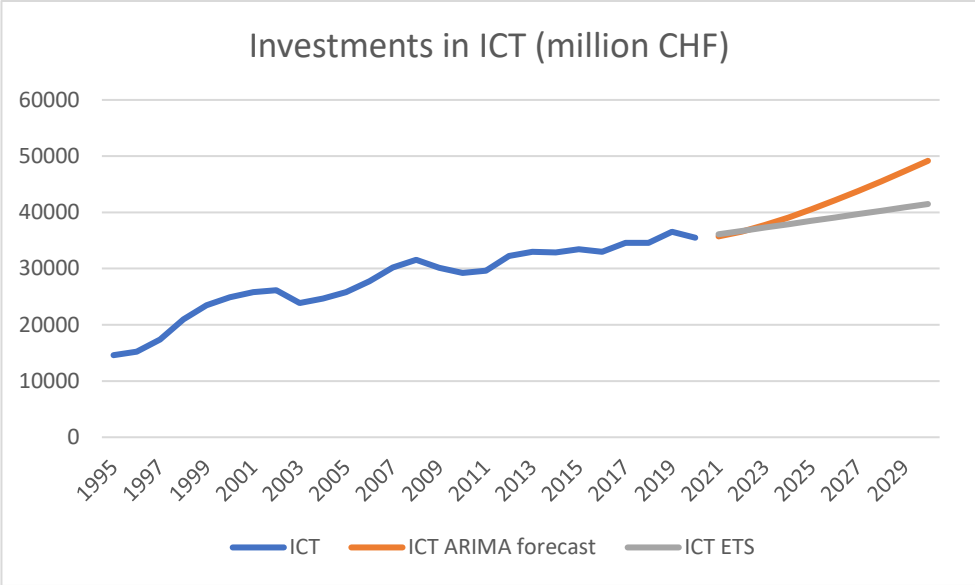
ARIMA Model Parameters

				Estimate	SE	t	Sig.
Y1_ICT-Model_1	Y1_ICT	Natural Logarithm	Constant	.034	.019	1.756	.092
			AR Lag 1	.461	.189	2.437	.023
			Difference	1			

The forecast using ETS shows the following results



Putting both forecast outcomes together for comparison give this final result. The values are in the table.



The forecast values using ARIMA and ETS. Hence that both forecasts have upper and lower bounds values.

Y1	ARIMA			ETS		
Year	Forecast	Upper	Lower	Forecast	Upper	Lower
2021	35726	31949	39836	36105.02	35503.93	35503.93
2022	36573	29950	44264	36702.48	33384.01	38826.04
2023	37745	28606	48971	37299.94	32663.43	40741.53
2024	39104	27686	53823	37897.4	32112.98	42486.91

2025	40583	27046	58786	38494.86	31626.74	44168.07
2026	42152	26600	63868	39092.32	31166.23	45823.50
2027	43798	26291	69089	39689.78	30713.03	47471.62
2028	45516	26085	74474	40287.24	30256.99	49122.58
2029	47305	25960	80047	40884.7	29792.05	50782.44
2030	49167	25899	85830	41482.16	29314.39	52455.01

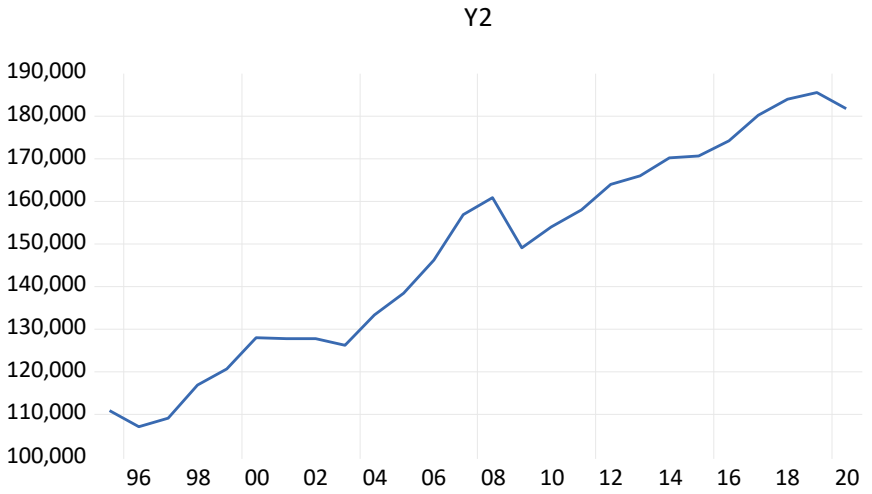
It is clear that both forecast methods suggest that the investments of ICT will continue to grow in the near future. This factor is a motivational engine for the digitalized society.

7.2.2 Modelling Gross Capital Formation (GCF) y2

The historic data from year 1995 through 2020 are published by FSO. The unit is million CHF (current)

Year	GCF	Year	GCF	Year	GCF
1995	111060	2004	133355	2013	165932
1996	107183	2005	138371	2014	170105
1997	109147	2006	146292	2015	170579
1998	116989	2007	156799	2016	174088
1999	120637	2008	160922	2017	180177
2000	128043	2009	149060	2018	183964
2001	127770	2010	153868	2019	185415
2002	127888	2011	157943	2020	181795
2003	126189	2012	163861		

The series is non-stationary based on the graph and the test



The test shows that the p-value is grater than 0.05, and the series has a unit root (non-stationary)

Null Hypothesis: Y2 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-0.661699	0.8389
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

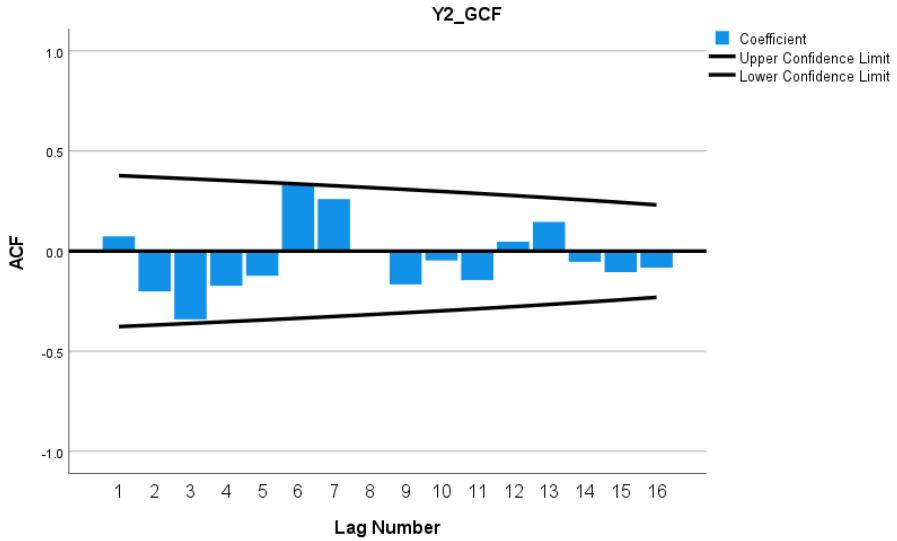
By taking the first difference, the series becomes stationary. The new p-value is lower than 0.05

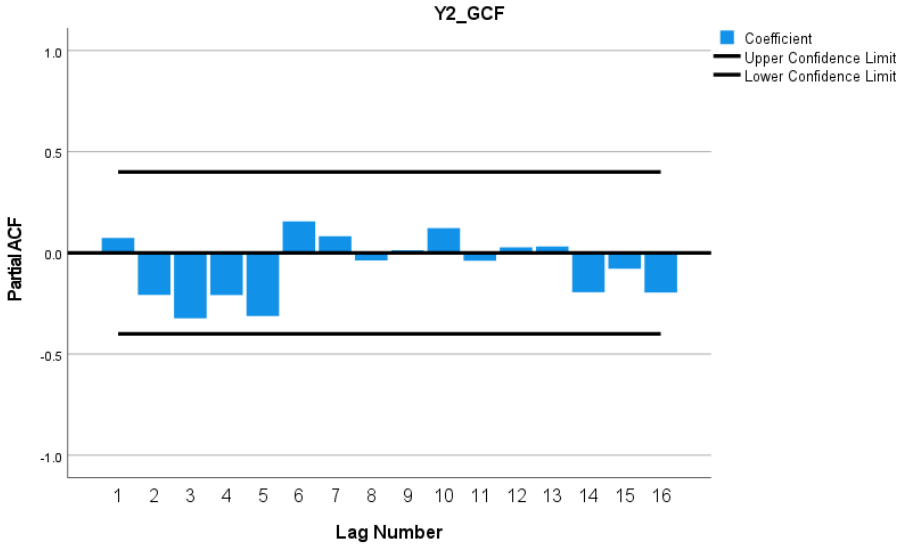
Null Hypothesis: D(Y2) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.455055	0.0019
Test critical values:	1% level	-3.737853	
	5% level	-2.991878	
	10% level	-2.635542	

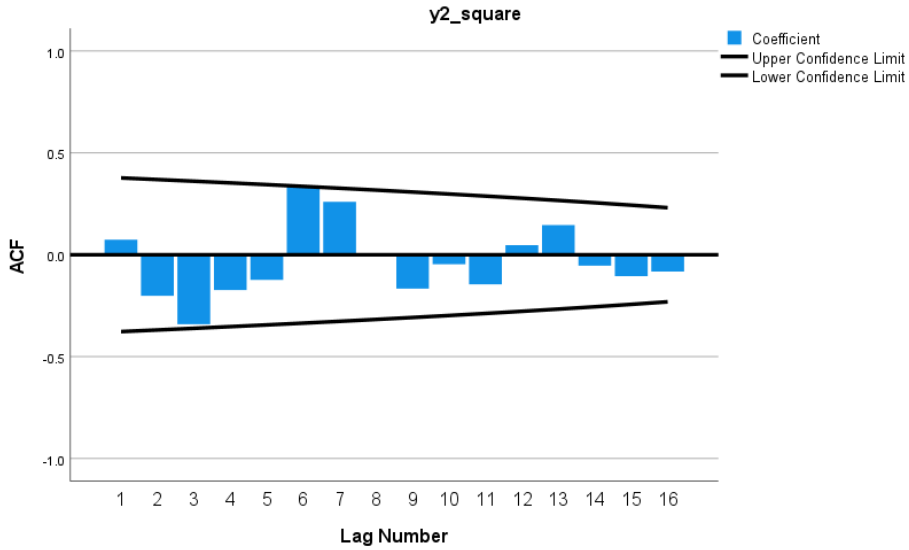
*MacKinnon (1996) one-sided p-values.

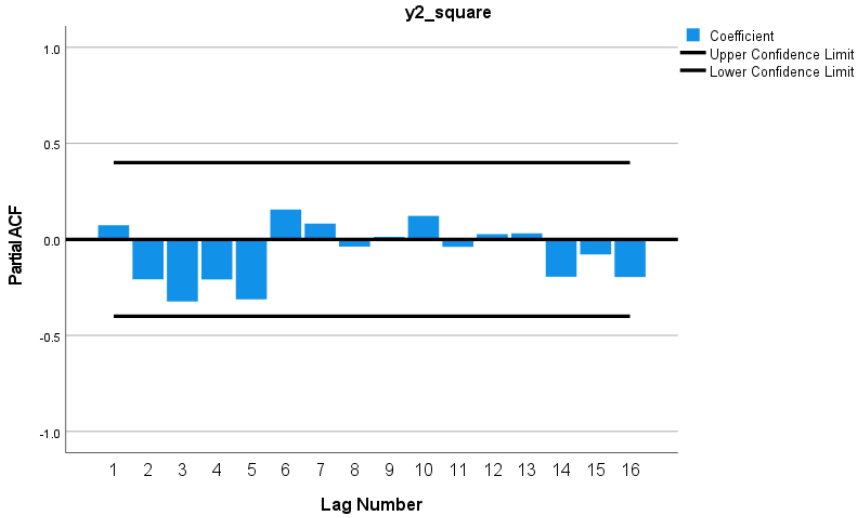
The correlogram for this series after taking the first difference and the logarithmic transfer shows that this series is not a standard AR process, and it is not a standard MA process. Therefore, it is not a directly identified ARIMA model.



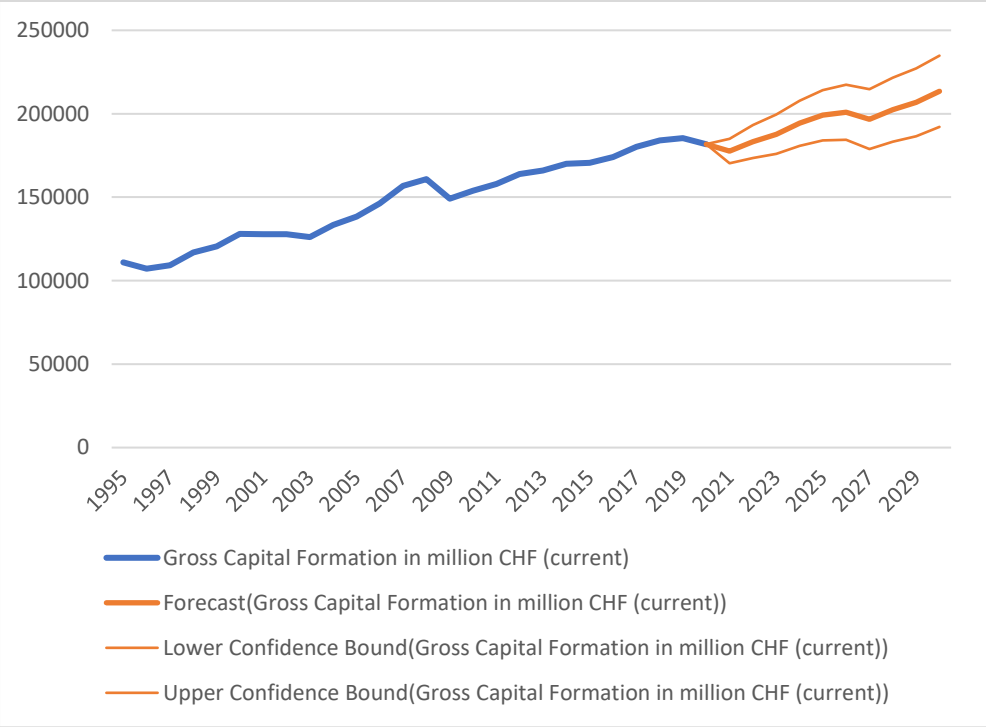


Even further transformation such as taking the square (see figure) of the data or taking the second difference, or dropping the logarithmic transfer give the same outcome that the series is not identified ARIMA model. However, it can be identified as ARIMA (0,1,0) but this has no significance. The only possibility is to forecast this series using the Exponential Smoothing ETS.





The forecast using Exponential Smoothing ETS is below



The values of the forecast

Year	Forecast	Lower Bound	Upper Bound
2021	177629	170336	184921
2022	183369	173552	193185
2023	187707	175890	199524
2024	194327	180799	207855
2025	199157	184108	214206
2026	200952	184519	217385
2027	196779	178786	214772
2028	202520	183349	221690
2029	206858	186576	227139
2030	213478	192140	234816

The investments in Gross Capital Formation will continue to increase in the next decade.

7.2.3 Modelling Gross Domestic Product GDP y3

This forecast was addressed in details as explanatory illustration for ARIMA model and for the Exponential Smoothing ETS.

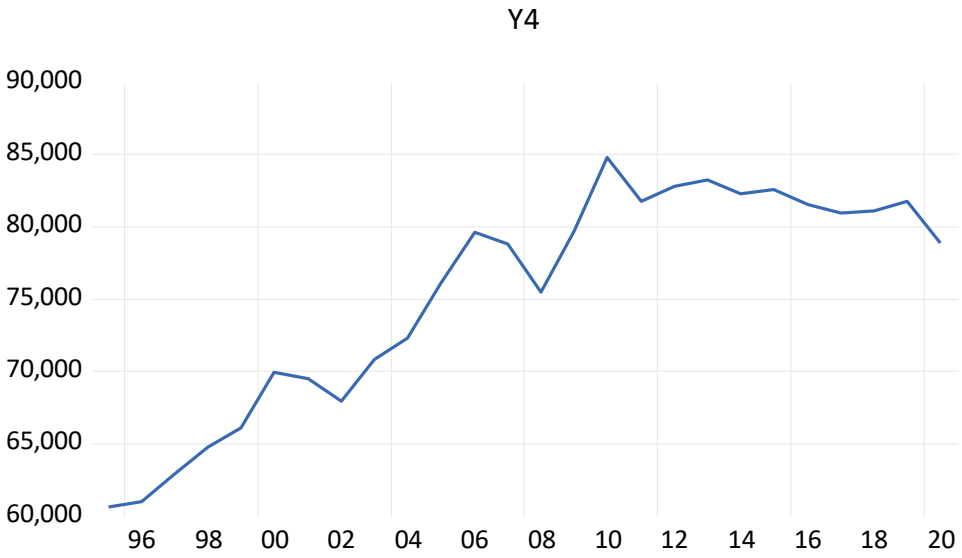
7.2.4 Modelling annual Gross National Income per Capita y4

This data is published by Worldbank. The unit is CHF (current).

Year	GNI	Year	GNI	Year	GNI
1995	60,611	2004	72,277	2013	83,256

1996	60,962	2005	76,035	2014	82,307
1997	62,928	2006	79,609	2015	82,591
1998	64,785	2007	78,775	2016	81,516
1999	66,097	2008	75,486	2017	80,965
2000	69,938	2009	79,717	2018	81,100
2001	69,508	2010	84,826	2019	81,755
2002	67,955	2011	81,763	2020	78,843
2003	70,797	2012	82,791		

To determine stationarity, the graph and the test are used.



The graph is not quite sufficient to determine stationarity despite that the series looks non-stationary.

The unit root test tells that it is non-stationary

Null Hypothesis: Y4 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.035815	0.2706
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

By taking the first difference, the test shows non-stationarity

Null Hypothesis: D(Y4) has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=5)

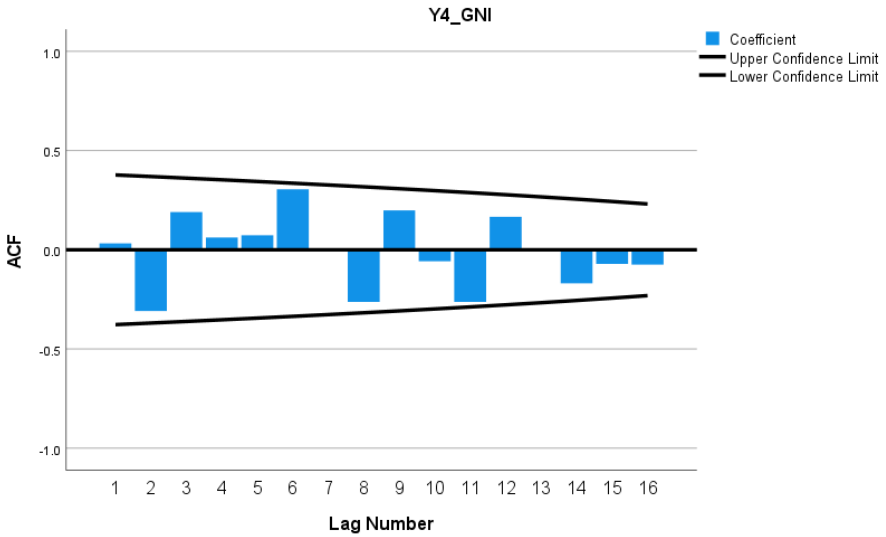
		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.397263	0.0023
Test critical values:	1% level	-3.752946	
	5% level	-2.998064	
	10% level	-2.638752	

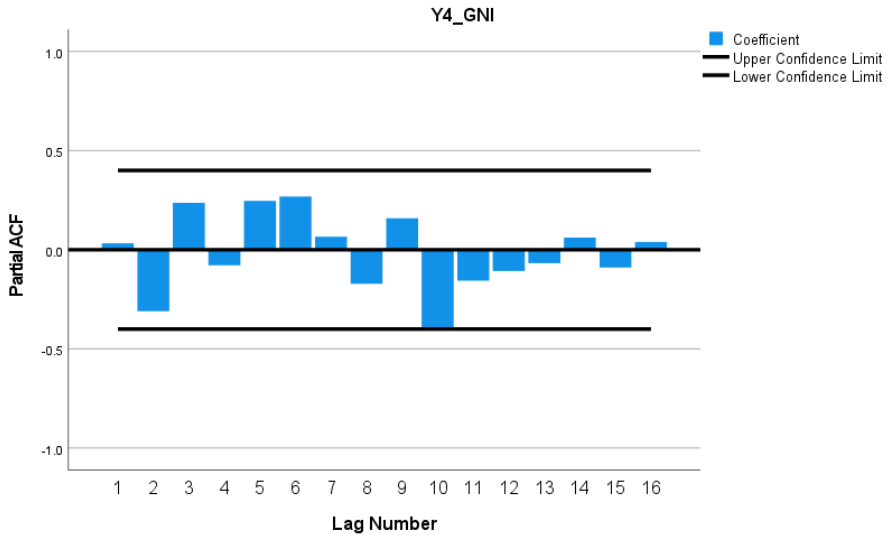
*MacKinnon (1996) one-sided p-values.

The correlogram for the PACF and ACF show that this series is neither an AR nor MA process. Therefore, it is not possible to use adequate ARIMA model for this forecast as it failed to identify the parameters p and q.

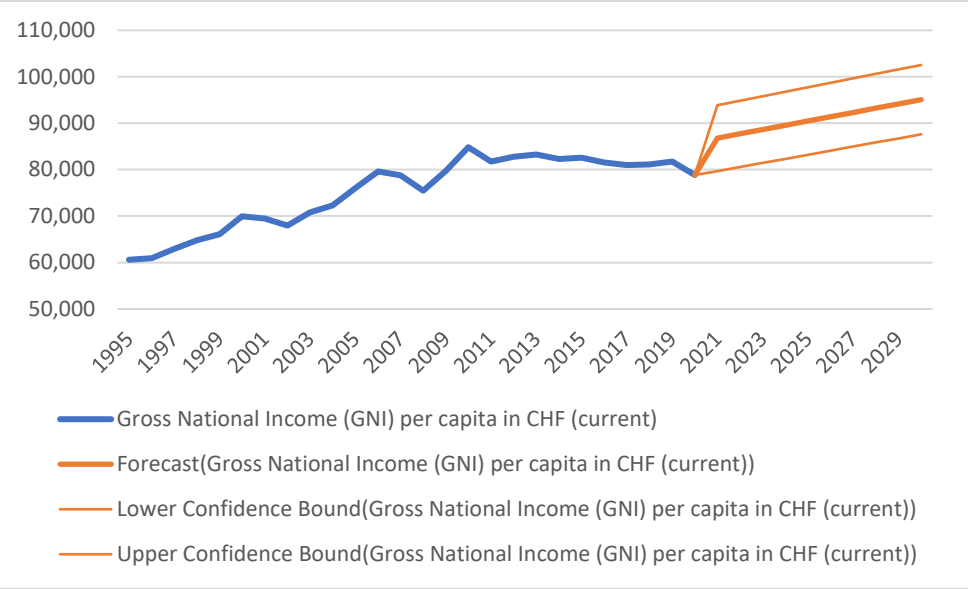
Taking the second difference and making other transformation does not improve the situation as the nature of this series is clearly not ARIMA process.

The sole possibility is to use the Exponential Smoothing ETS.





The forecast using the Exponential Smoothing ETS shows that the GNI will increase for the coming decade.



The forecasted values are in the table

Year	Forecast	Lower Bound	Upper Bound
2021	86,794	79,680	93,908
2022	87,714	80,564	94,863
2023	88,633	81,446	95,820
2024	89,553	82,329	96,776
2025	90,472	83,210	97,734
2026	91,392	84,092	98,692
2027	92,311	84,972	99,650
2028	93,231	85,852	100,609
2029	94,150	86,732	101,568
2030	95,070	87,611	102,528

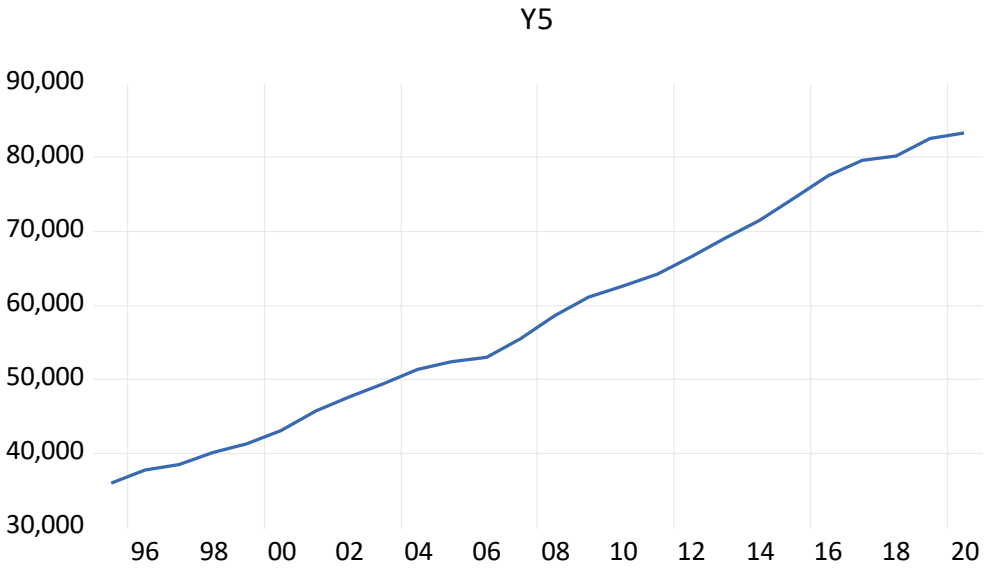
7.2.5 Modelling healthcare costs y5

The historic data is published by FSO. The unit is million current CHF.

Year	Healthcare Costs	Year	Healthcare Costs	Year	Healthcare Costs
1995	36,056	2004	51,361	2013	69,118
1996	37,773	2005	52,388	2014	71,429
1997	38,544	2006	53,048	2015	74,385
1998	40,077	2007	55,474	2016	77,455
1999	41,330	2008	58,563	2017	79,643
2000	43,072	2009	61,157	2018	80,242
2001	45,754	2010	62,565	2019	82,472

2002	47,629	2011	64,243	2020	83,311
2003	49,429	2012	66,512		

The graph shows that the series is non-stationary.



The unit root test confirms the result.

Null Hypothesis: Y5 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		0.874228	0.9933
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

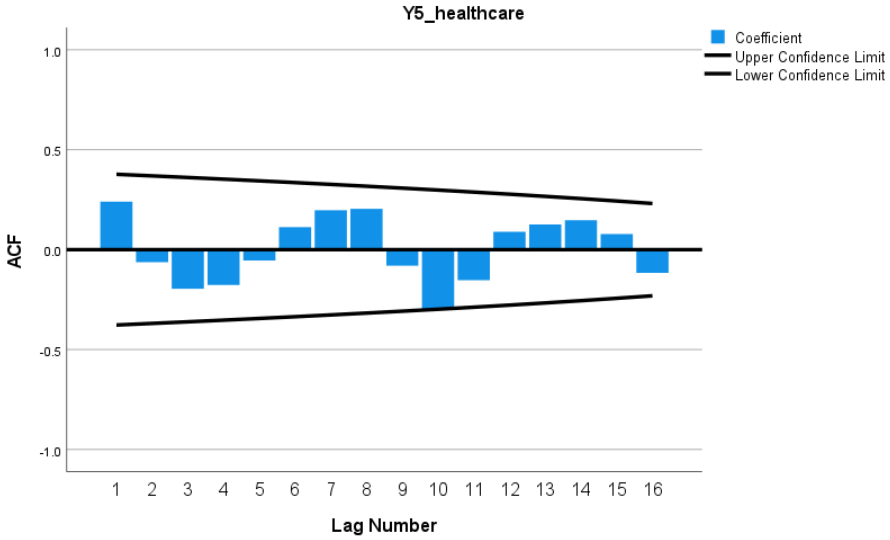
By taking the first order difference, the series becomes stationary.

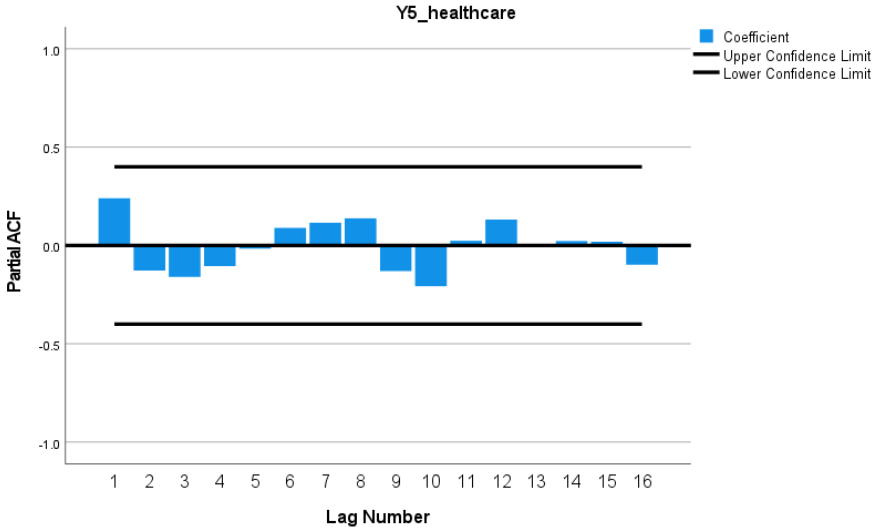
Null Hypothesis: D(Y5) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-3.272353	0.0279
Test critical values:	1% level	-3.737853	
	5% level	-2.991878	
	10% level	-2.635542	

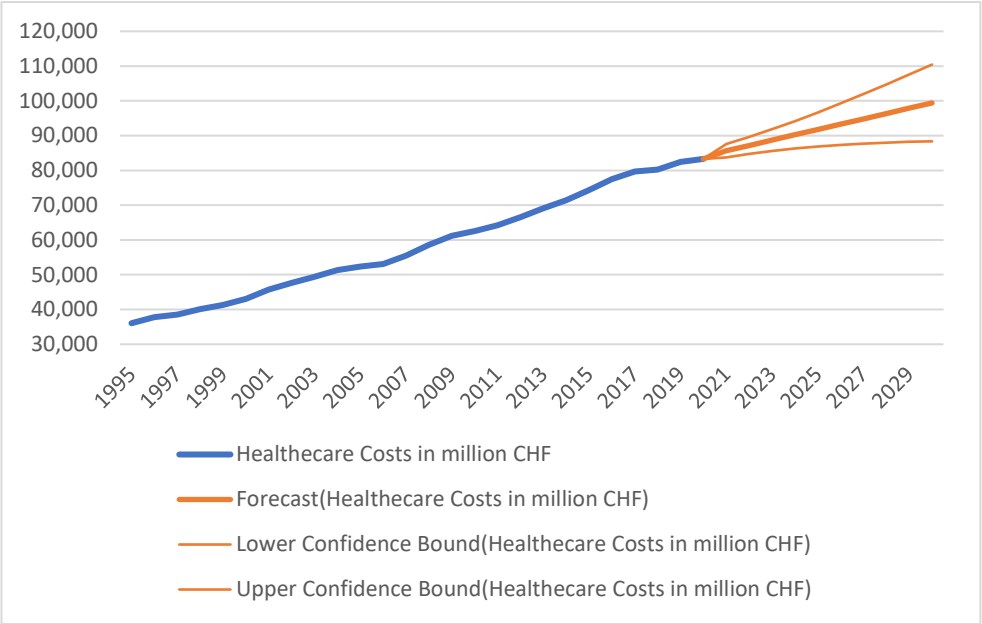
*MacKinnon (1996) one-sided p-values.

The correlogram of the logarithmic transformation shows that the series is not an AR process nor MA process. Therefore, it is only possible to use the Exponential Smoothing ETS.





The Exponential Smoothing ETS forecast is below



The forecast shows that the expenses will keep increasing for the near future. The values of the forecast are in the table.

Year	Forecast	Lower Bound	Upper Bound
2021	85,645	83,703	87,587
2022	87,174	84,746	89,601
2023	88,702	85,593	91,811
2024	90,231	86,286	94,175
2025	91,759	86,855	96,663

2026	93,287	87,321	99,254
2027	94,816	87,696	101,936
2028	96,344	87,991	104,698
2029	97,873	88,210	107,535
2030	99,401	88,361	110,442

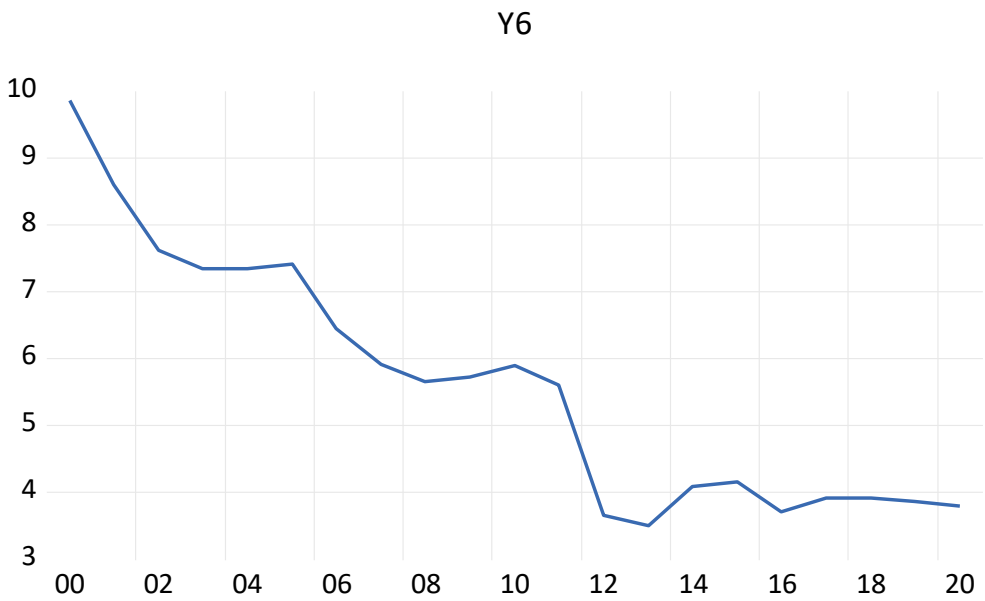
7.2.6 Modelling ICT Goods Import y6

The data is published by the Worldbank. It is only available through the years 2000 and 2020. The less entries for ARIMA models give less quality forecast. But the forecast still serves the purpose of this dissertation.

This variable reflects the ICT goods imports as percentage of the total good imports.

Year	ICT imports	Year	ICT imports
2000	9.85	2011	5.59
2001	8.59	2012	3.65
2002	7.62	2013	3.50
2003	7.33	2014	4.08
2004	7.33	2015	4.14
2005	7.41	2016	3.69
2006	6.44	2017	3.91
2007	5.91	2018	3.91
2008	5.65	2019	3.85
2009	5.72	2020	3.78

The graph shows that the series is non-stationary.



The unit root test confirms the result as well.

Null Hypothesis: Y6 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=4)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.623291	0.1050
Test critical values:	1% level	-3.808546	
	5% level	-3.020686	
	10% level	-2.650413	

*MacKinnon (1996) one-sided p-values.

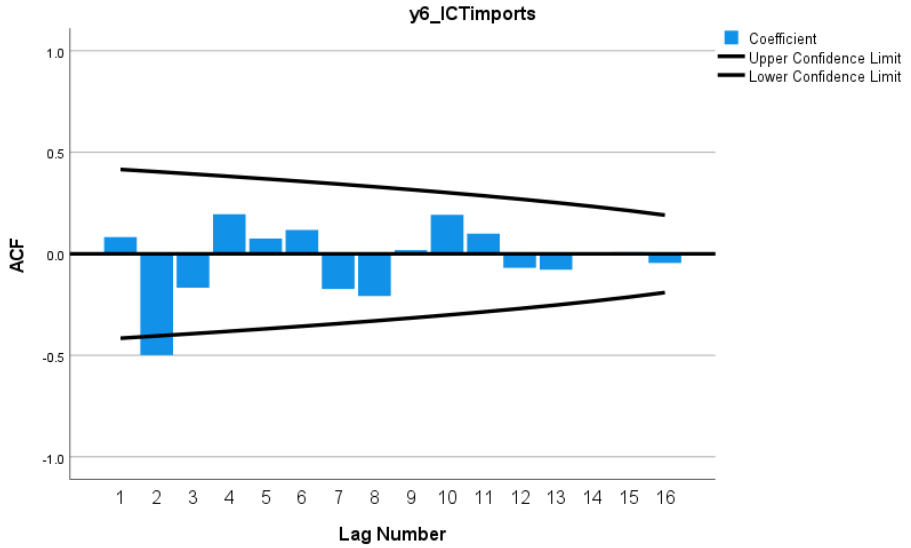
After taking the first difference, the series is stationary.

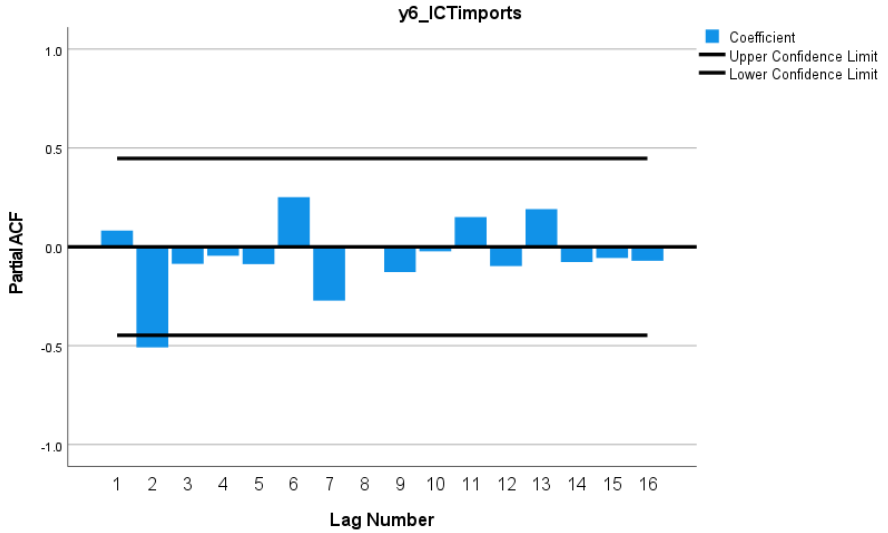
Null Hypothesis: D(Y6) has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=4)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.569423	0.0024
Test critical values:	1% level	-3.857386	
	5% level	-3.040391	
	10% level	-2.660551	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 18

The correlogram of the PACF and ACF gives the following results





There is a clear cut-off for both functions at the second lag. So that the suggested parameters for p and q is 2.

The considered ARIMA models in this case are: ARIMA (2,1,2), ARIMA (2,1,0), and ARIMA (0,1,2).

The coefficients for lags 1 and 3 are very low, therefore the considered parameters will not extend the outcomes of the functions.

ARIMA (2,1,2) as shown below is not a good model. The p-values for the constant, AR, and MA are greater than 0.05

Dependent Variable: D(LY6)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 16:46
Sample: 2001 2020
Included observations: 20
Convergence achieved after 14 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.046338	0.027791	-1.667396	0.1149
AR(2)	-0.414845	1.611742	-0.257389	0.8002
MA(2)	-0.096200	1.403784	-0.068529	0.9462
SIGMASQ	0.009008	0.002703	3.332026	0.0042

R-squared	0.266903	Mean dependent var	-0.047887
Adjusted R-squared	0.129447	S.D. dependent var	0.113729
S.E. of regression	0.106113	Akaike info criterion	-1.444119
Sum squared resid	0.180161	Schwarz criterion	-1.244972
Log likelihood	18.44119	Hannan-Quinn criter.	-1.405243
F-statistic	1.941739	Durbin-Watson stat	1.845138
Prob(F-statistic)	0.163570		

Inverted AR Roots	-.00+.64i	-.00-.64i
Inverted MA Roots	.31	-.31

ARIMA (0,1,2) is also not a suitable model. As the p-value for MA is greater than 0.05

Dependent Variable: D(LY6)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 16:53
Sample: 2001 2020
Included observations: 20
Convergence achieved after 7 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.047515	0.023049	-2.061512	0.0549
MA(2)	-0.413475	0.357964	-1.155073	0.2640
SIGMASQ	0.009618	0.002609	3.686224	0.0018

R-squared	0.217292	Mean dependent var	-0.047887
Adjusted R-squared	0.125209	S.D. dependent var	0.113729
S.E. of regression	0.106371	Akaike info criterion	-1.487531
Sum squared resid	0.192353	Schwarz criterion	-1.338171
Log likelihood	17.87531	Hannan-Quinn criter.	-1.458374
F-statistic	2.359737	Durbin-Watson stat	1.930233
Prob(F-statistic)	0.124623		

Inverted MA Roots	.64	-.64

ARIMA (2,1,0) is not a suitable model either. The p-value for AR is greater than 0.05.

Dependent Variable: D(LY6)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 16:55
Sample: 2001 2020
Included observations: 20
Convergence achieved after 4 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.046165	0.028142	-1.640395	0.1193
AR(2)	-0.482610	0.595564	-0.810342	0.4289
SIGMASQ	0.009057	0.002661	3.403659	0.0034

R-squared	0.262921	Mean dependent var	-0.047887
Adjusted R-squared	0.176206	S.D. dependent var	0.113729
S.E. of regression	0.103224	Akaike info criterion	-1.539828
Sum squared resid	0.181139	Schwarz criterion	-1.390469
Log likelihood	18.39828	Hannan-Quinn criter.	-1.510672
F-statistic	3.032010	Durbin-Watson stat	1.818097
Prob(F-statistic)	0.074794		

Inverted AR Roots	-.00+.69i	-.00-.69i

Despite the ability to identify parameters for the ARIMA model, ARIMA is not suitable for this forecast.

The forecast using Exponential Smoothing ETS estimates that ICT import % will be around 4% for the coming decade. The results of the forecast are presented.

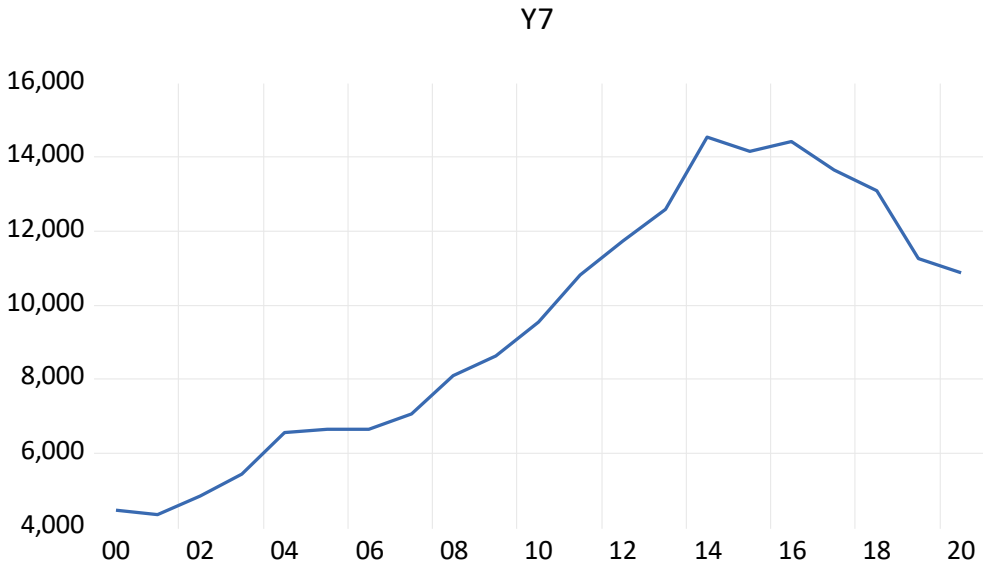
Year	Forecast	Lower Bound	Upper Bound
2021	3.56	2.10	5.03
2022	3.61	2.10	5.12
2023	3.66	2.05	5.26
2024	3.70	1.94	5.47
2025	3.75	1.76	5.74
2026	3.80	1.52	6.07
2027	3.84	1.23	6.45
2028	3.89	0.90	6.88
2029	3.94	0.52	7.35
2030	3.98	0.10	7.86

7.2.7 Modelling ICT services exports

The historic data are available from year 1977 until year 2020 and is published by the Worldbank. The unit used is the US dollar (current). However, there is an interesting observation about the numbers. The figure for year 1999 was 840 million USD, and for year 2000 it jumped to 4'450 million USD which 5 times more than the previous year. The only explanation for this radical increase in exports is the redefinition of ICT goods. So that new type of services became included from year 2000 onwards. The complete data is presented, but only the entries from year 2000 will be considered for the modelling because the homogeneity of the data is very important.

Year	ICT exports	Year	ICT exports	Year	ICT exports	Year	ICT exports
1977	129	1988	401	1999	843	2010	9,548
1978	143	1989	346	2000	4,452	2011	10,811
1979	156	1990	424	2001	4,349	2012	11,725
1980	122	1991	406	2002	4,840	2013	12,581
1981	148	1992	481	2003	5,427	2014	14,541
1982	163	1993	454	2004	6,551	2015	14,167
1983	170	1994	466	2005	6,636	2016	14,420
1984	177	1995	526	2006	6,648	2017	13,643
1985	216	1996	516	2007	7,067	2018	13,086
1986	340	1997	489	2008	8,095	2019	11,270
1987	424	1998	623	2009	8,638	2020	10,877

The variable plot shows that the series is non-stationary. The same result is confirmed by the unit root test.



Null Hypothesis: Y7 has a unit root
Exogenous: Constant
Lag Length: 2 (Automatic - based on SIC, maxlag=4)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.108971	0.2435
Test critical values:	1% level	-3.857386	
	5% level	-3.040391	
	10% level	-2.660551	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 18

By taking the first order difference, the series is still non-stationary, as the p-value is 0.81 is higher than 0.05.

Null Hypothesis: D(Y7) has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=4)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-0.734215	0.8134
Test critical values:	1% level	-3.857386	
	5% level	-3.040391	
	10% level	-2.660551	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 18

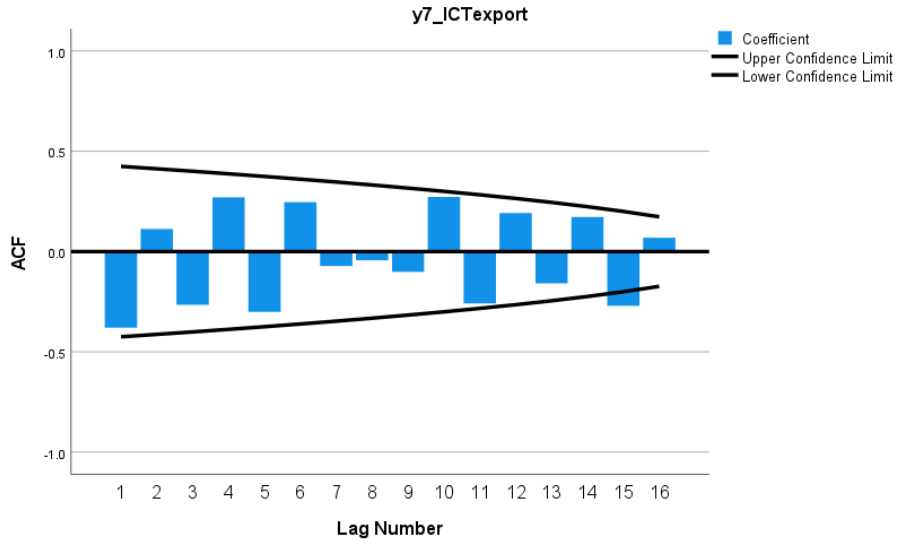
The series becomes stationary only after taking the second difference. The ARIMA parameter $D = 2$.

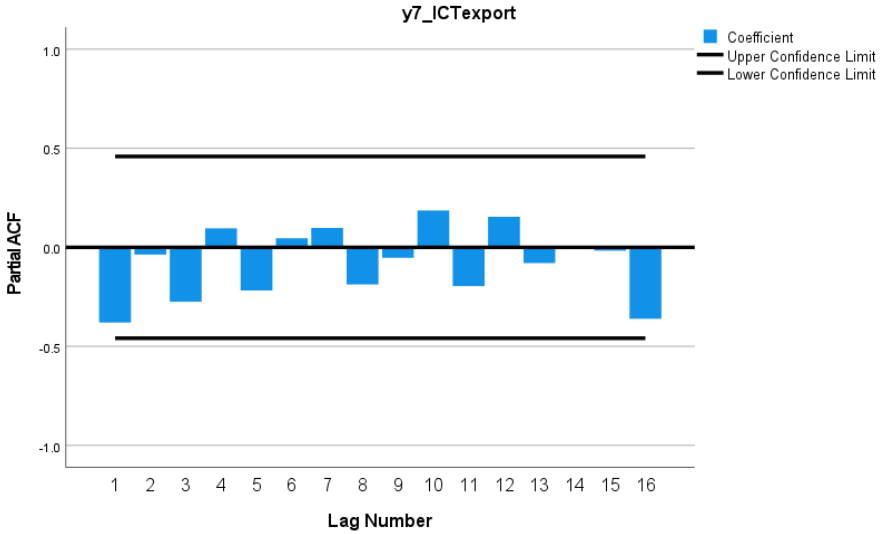
Null Hypothesis: D(Y7,2) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=4)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-7.433984	0.0000
Test critical values:	1% level	-3.857386	
	5% level	-3.040391	
	10% level	-2.660551	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 18

The analysis of the correlogram give the following outcomes.





There is no clear cut-off at either of the PACF and the ACF. However, the coefficient of the correlation is very close to the cut-off at the first lag for both functions. Therefore, the value 1 will be considered for both parameters p and q.

The possible ARIMA models are: ARIMA (1,2,1), ARIMA (1,2,0), and ARIMA (0,2,1).

ARIMA (1,2,1) is not a good model. The p-values are higher than 0.05

Dependent Variable: D(LY7,2)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 17:58
Sample: 2002 2020
Included observations: 19
Failure to improve objective (non-zero gradients) after 105 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.006650	0.005955	-1.116779	0.2817
AR(1)	0.309346	0.454667	0.680380	0.5066
MA(1)	-1.000000	9915.025	-0.000101	0.9999
SIGMASQ	0.004904	1.077715	0.004551	0.9964

R-squared	0.325263	Mean dependent var	-0.000640
Adjusted R-squared	0.190315	S.D. dependent var	0.087592
S.E. of regression	0.078817	Akaike info criterion	-1.932396
Sum squared resid	0.093182	Schwarz criterion	-1.733567
Log likelihood	22.35776	Hannan-Quinn criter.	-1.898746
F-statistic	2.410293	Durbin-Watson stat	1.789043
Prob(F-statistic)	0.107477		

Inverted AR Roots	.31
Inverted MA Roots	1.00

ARIMA (0,2,1) is also not a good model for the same reason.

Dependent Variable: D(LY7,2)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 18:00
Sample: 2002 2020
Included observations: 19
Convergence achieved after 11 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.006981	0.007718	-0.904517	0.3791
MA(1)	-0.625951	0.218769	-2.861238	0.0113
SIGMASQ	0.005510	0.002725	2.021596	0.0603

R-squared	0.241986	Mean dependent var	-0.000640
Adjusted R-squared	0.147234	S.D. dependent var	0.087592
S.E. of regression	0.080887	Akaike info criterion	-2.021418
Sum squared resid	0.104683	Schwarz criterion	-1.872296
Log likelihood	22.20347	Hannan-Quinn criter.	-1.996181
F-statistic	2.553889	Durbin-Watson stat	1.666966
Prob(F-statistic)	0.108998		

Inverted MA Roots	.63

ARIMA (1,2,0) is also not a good model because the p-value for the constant is higher than 0.05.

This analysis means that ARIMA is not suitable to model this time series. If one looks at the series plot, it is noticeable that it has linear increase until it reaches its peak before it drops linearly. This shape is not typically suitable for ARIMA models. Nevertheless, a confirmation using statistical analysis was additional prove that ARIMA is not suitable for this series.

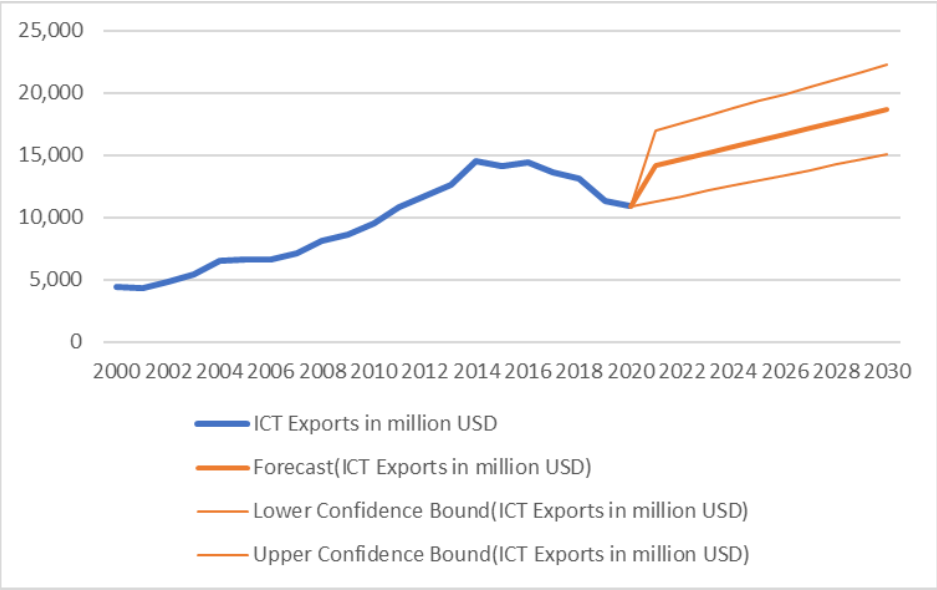
Dependent Variable: D(LY7,2)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/09/22 Time: 18:00
Sample: 2002 2020
Included observations: 19
Convergence achieved after 11 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-0.006981	0.007718	-0.904517	0.3791
MA(1)	-0.625951	0.218769	-2.861238	0.0113
SIGMASQ	0.005510	0.002725	2.021596	0.0603

R-squared	0.241986	Mean dependent var	-0.000640
Adjusted R-squared	0.147234	S.D. dependent var	0.087592
S.E. of regression	0.080887	Akaike info criterion	-2.021418
Sum squared resid	0.104683	Schwarz criterion	-1.872296
Log likelihood	22.20347	Hannan-Quinn criter.	-1.996181
F-statistic	2.553889	Durbin-Watson stat	1.666966
Prob(F-statistic)	0.108998		

Inverted MA Roots	.63

This variable will be forecasted using the Exponential Smoothing ETS. The results and forecasted numbers are presented.



The forecast expects the figure for the exported ICT services to increase during the coming decade.

The table shows the forecast together with the upper and lower bounds.

Year	Forecast	Lower Bound	Upper Bound
2021	14,129	11,285	16,973
2022	14,634	11,702	17,567
2023	15,140	12,121	18,159
2024	15,646	12,542	18,749
2025	16,151	12,965	19,337
2026	16,657	13,389	19,925
2027	17,162	13,814	20,510
2028	17,668	14,241	21,095
2029	18,173	14,669	21,678
2030	18,679	15,098	22,260

7.2.8 Modelling medium and high-tech exports y8

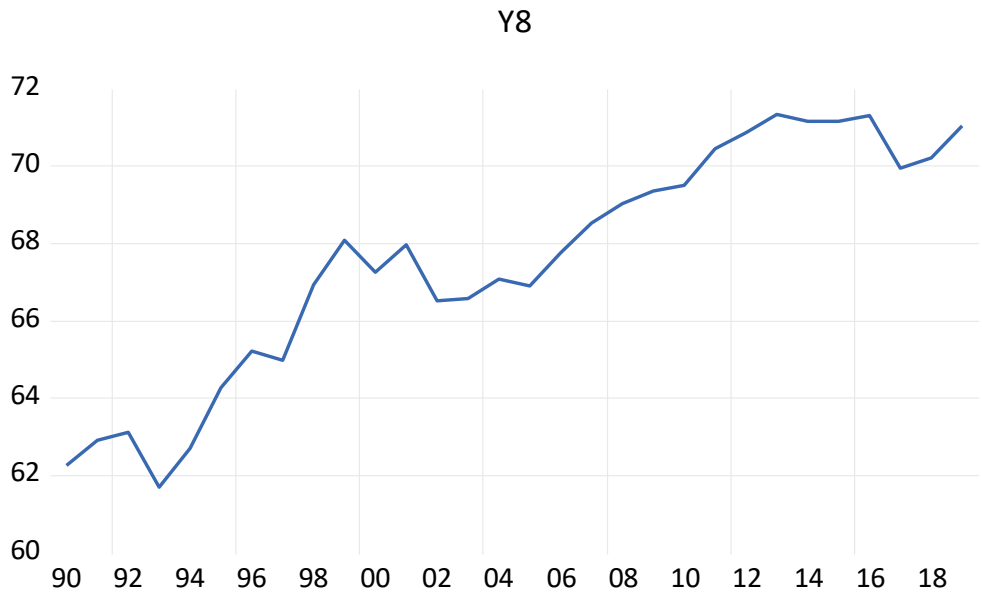
This variable is about the figure of medium and high-tech exports (% manufactured exports). The historic data is published by the Worldbank.

Year	Value	Year	Value	Year	Value
1990	62.27	2000	67.24	2010	69.50
1991	62.91	2001	67.96	2011	70.45
1992	63.13	2002	66.52	2012	70.87
1993	61.69	2003	66.59	2013	71.33

1994	62.72	2004	67.07	2014	71.14
1995	64.26	2005	66.91	2015	71.15
1996	65.21	2006	67.75	2016	71.31
1997	64.99	2007	68.53	2017	69.95
1998	66.93	2008	69.02	2018	70.20
1999	68.10	2009	69.35	2019	71.03

This variable reflects into a certain limit the dependence of Swiss exports on medium and high-tech goods. That is why it is very important for the economy and for the forecast.

The plot of y8 shows that the series is not stationary. The unit root test shows the same result.



Taking the first order difference makes the series stationary.

Null Hypothesis: Y8 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-1.365850	0.5848
Test critical values:	1% level	-3.679322	
	5% level	-2.967767	
	10% level	-2.622989	

*MacKinnon (1996) one-sided p-values.

Null Hypothesis: D(Y8) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

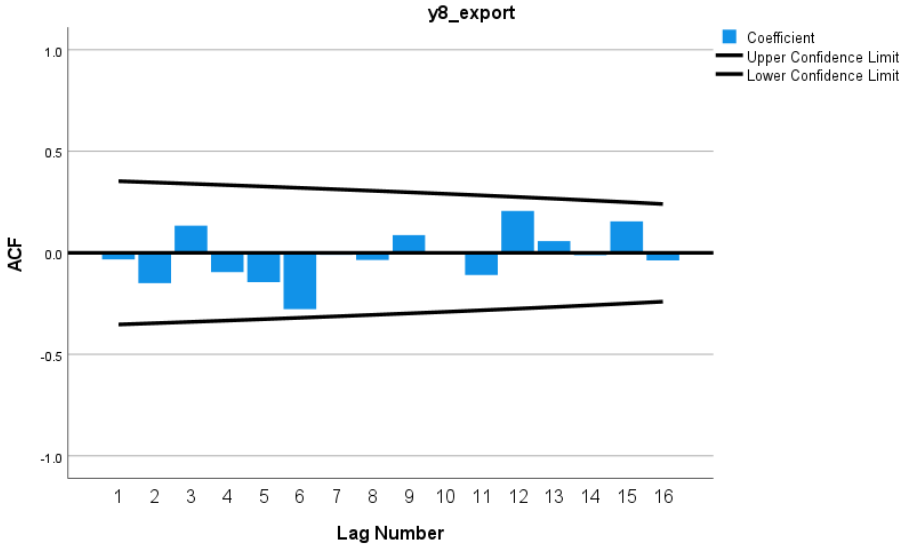
		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-5.257494	0.0002
Test critical values:	1% level	-3.689194	
	5% level	-2.971853	
	10% level	-2.625121	

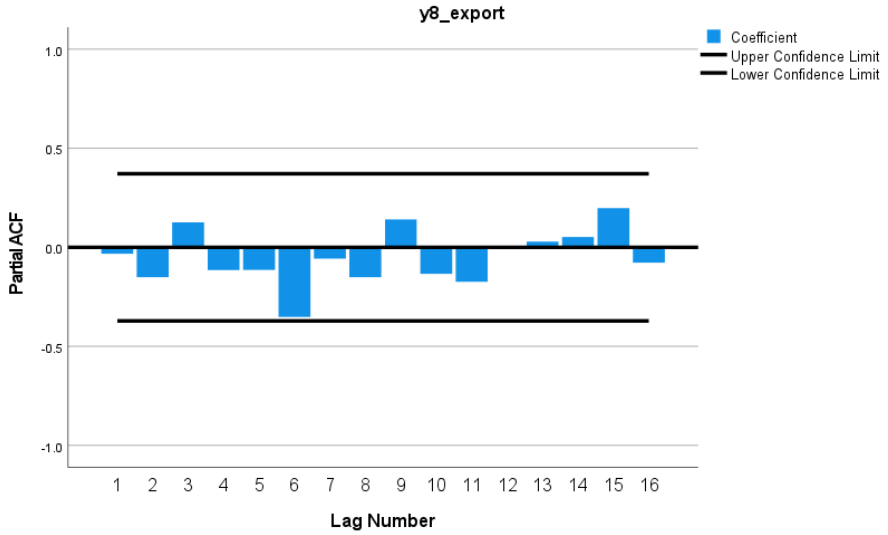
*MacKinnon (1996) one-sided p-values.

The correlogram analysis fail to identify parameters for the ARIMA models.

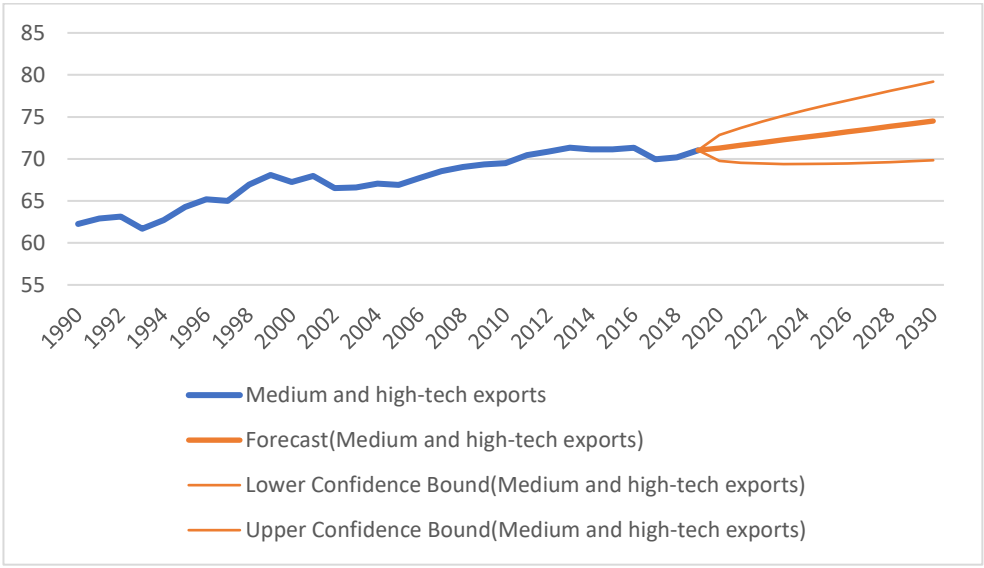
The series is not an AR process nor MA process.

The only option remaining is using the Exponential Smoothing ETS.





The outcomes of the forecast and the values are presented.



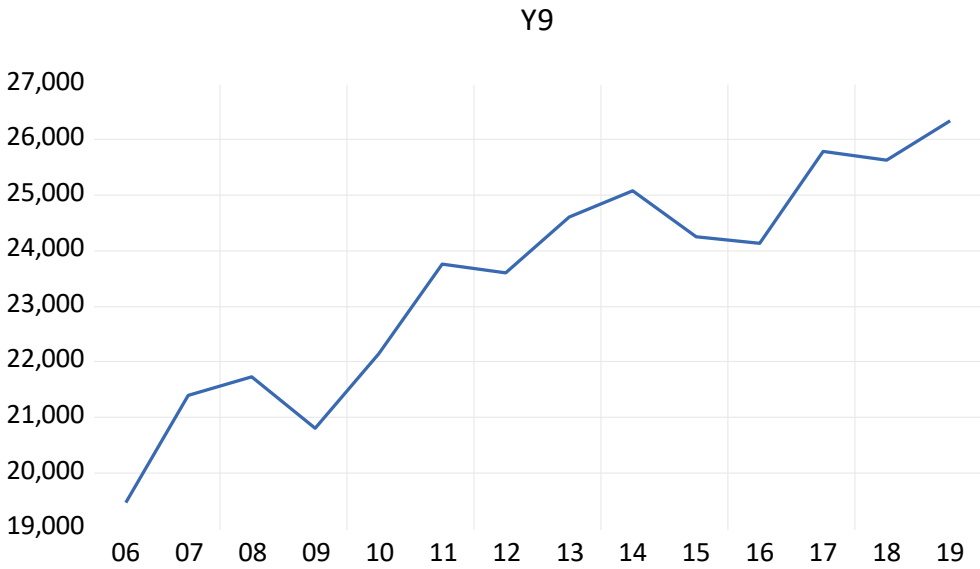
Year	Forecast	Lower Bond	Upper Bound
2020	71.30	69.76	72.85
2021	71.63	69.55	73.71
2022	71.95	69.44	74.45
2023	72.27	69.40	75.13
2024	72.59	69.40	75.78
2025	72.91	69.43	76.39
2026	73.23	69.47	76.98
2027	73.55	69.54	77.56
2028	73.87	69.62	78.11
2029	74.19	69.72	78.66
2030	74.51	69.82	79.20

The medium and high-tech exports as percentage of manufactured exports are expected to increase for the coming years. Unfortunately, the data for the years 2020 and 2021 are not available, but this should not affect the quality of the forecast.

7.2.9 Modelling new registered business y9

The data is only available from year 2006 through year 2019 and is published by the Worldbank. There are no enough entries for a proper ARIMA forecast.

The plot shows that the series is non-stationary. But it becomes stationary after taking the first difference.



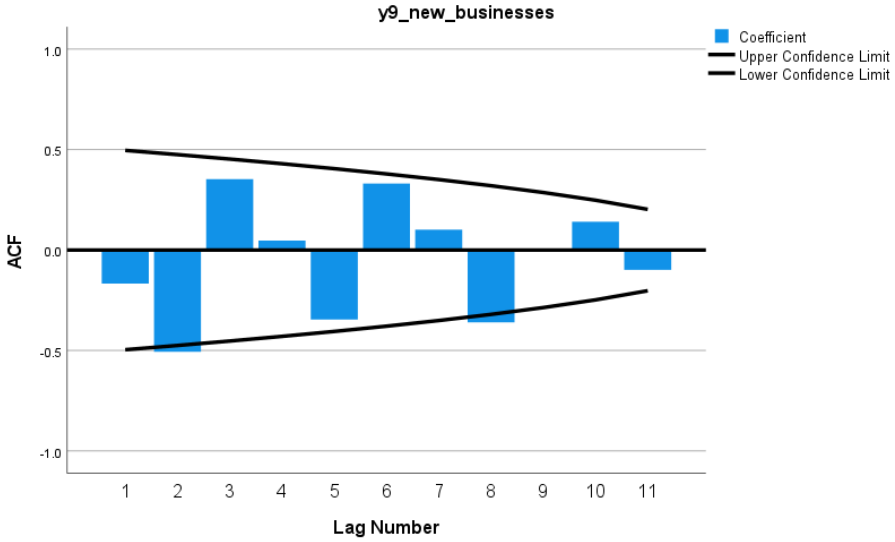
The unit root test for the first difference is presented

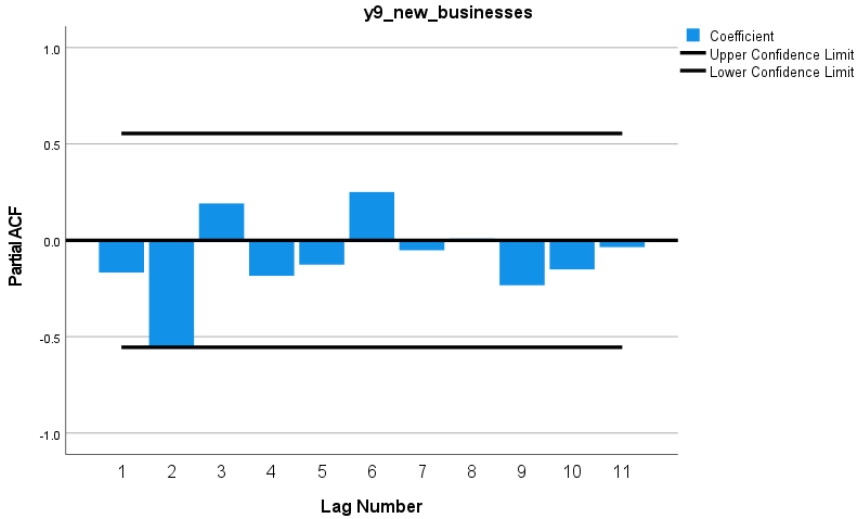
Null Hypothesis: D(Y9) has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=2)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.795645	0.0041
Test critical values:	1% level	-4.200056	
	5% level	-3.175352	
	10% level	-2.728985	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 11

The correlogram of the PACF and the ACF shows the following results





The possible parameters for ARIMA model are D=1, p=2, q=2.

The potential models are ARIMA (2,1,2), ARIMA (0,1,2), and ARIMA (2,1,0).

ARIMA (2,1,2) is a bad fit for the series because the p-values for the coefficients are higher than 0.05

Dependent Variable: D(LY9)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/10/22 Time: 12:02
Sample: 2007 2019
Included observations: 13
Failure to improve objective (non-zero gradients) after 23 iterations
Coefficient covariance computed using outer product of gradients
d.f. adjustment for standard errors & covariance

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.023435	0.013819	1.695853	0.1241
AR(2)	-0.932137	3.036940	-0.306933	0.7659
MA(2)	1.000000	4641.342	0.000215	0.9998
SIGMASQ	0.001573	3.645583	0.000431	0.9997

R-squared	0.039423	Mean dependent var	0.023264
Adjusted R-squared	-0.280770	S.D. dependent var	0.042115
S.E. of regression	0.047662	Akaike info criterion	-2.970091
Sum squared resid	0.020445	Schwarz criterion	-2.796260
Log likelihood	23.30559	Hannan-Quinn criter.	-3.005821
F-statistic	0.123122	Durbin-Watson stat	2.088327
Prob(F-statistic)	0.944108		

Inverted AR Roots	-.00+.97i	-.00-.97i
Inverted MA Roots	-.00+1.00i	-.00-1.00i

ARIMA (0,1,2) is also not a good model for the same reason.

Dependent Variable: D(LY9)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/10/22 Time: 12:07
Sample: 2007 2019
Included observations: 13
Convergence achieved after 23 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.022080	0.004536	4.867384	0.0007
MA(2)	-0.679713	0.432196	-1.572694	0.1469
SIGMASQ	0.001023	0.000619	1.651550	0.1296

R-squared	0.375272	Mean dependent var	0.023264
Adjusted R-squared	0.250326	S.D. dependent var	0.042115
S.E. of regression	0.036465	Akaike info criterion	-3.490910
Sum squared resid	0.013297	Schwarz criterion	-3.360537
Log likelihood	25.69091	Hannan-Quinn criter.	-3.517707
F-statistic	3.003482	Durbin-Watson stat	2.095732
Prob(F-statistic)	0.095160		

Inverted MA Roots	.82	-.82

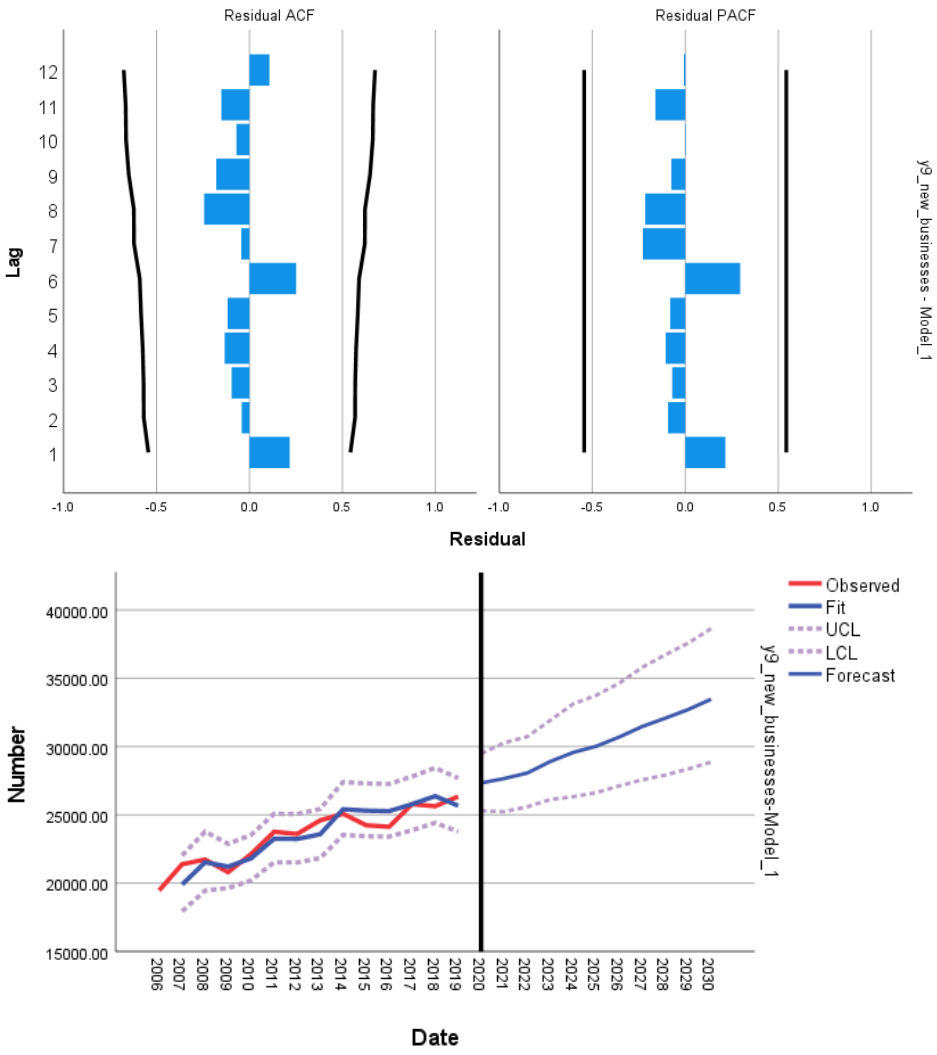
ARIMA (2,1,0) might be a suitable model for the series

Dependent Variable: D(LY9)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/10/22 Time: 12:05
Sample: 2007 2019
Included observations: 13
Convergence achieved after 9 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.022042	0.006586	3.346986	0.0074
AR(2)	-0.583693	0.252599	-2.310745	0.0435
SIGMASQ	0.001069	0.000640	1.670659	0.1257

R-squared	0.347291	Mean dependent var	0.023264
Adjusted R-squared	0.216749	S.D. dependent var	0.042115
S.E. of regression	0.037272	Akaike info criterion	-3.477872
Sum squared resid	0.013892	Schwarz criterion	-3.347499
Log likelihood	25.60617	Hannan-Quinn criter.	-3.504669
F-statistic	2.660378	Durbin-Watson stat	1.960993
Prob(F-statistic)	0.118467		

Inverted AR Roots	-.00+.76i	-.00-.76i

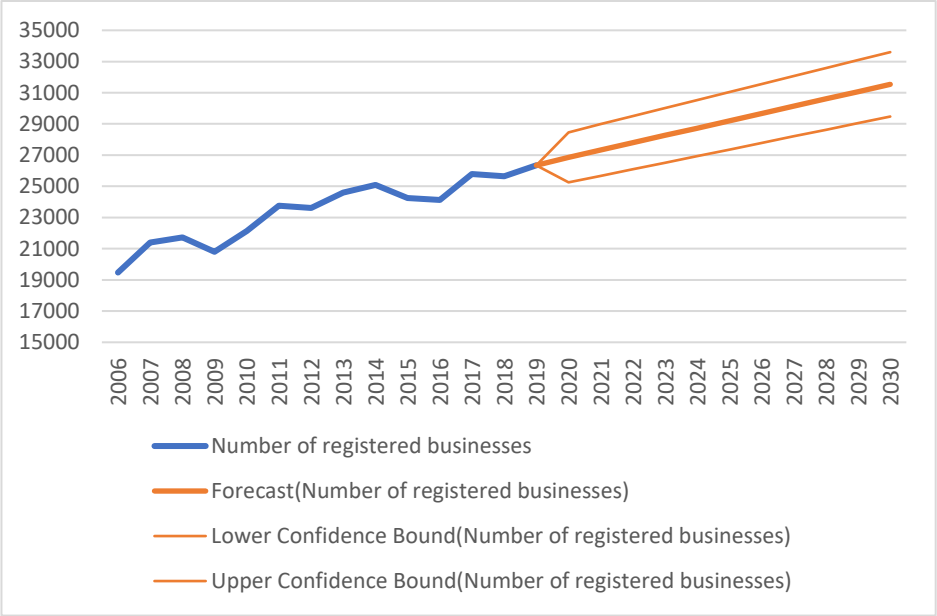


The model ARIMA (2,1,0) is selected. The correlogram of the residuals shows only white noise. This means that the model is suitable.

The forecast results and the values are presented. It suggests that the number of the new registered businesses will continue to increase. Nevertheless, one must not forget that this is only predictions based on historic data and on ongoing economic situation and economy crisis.

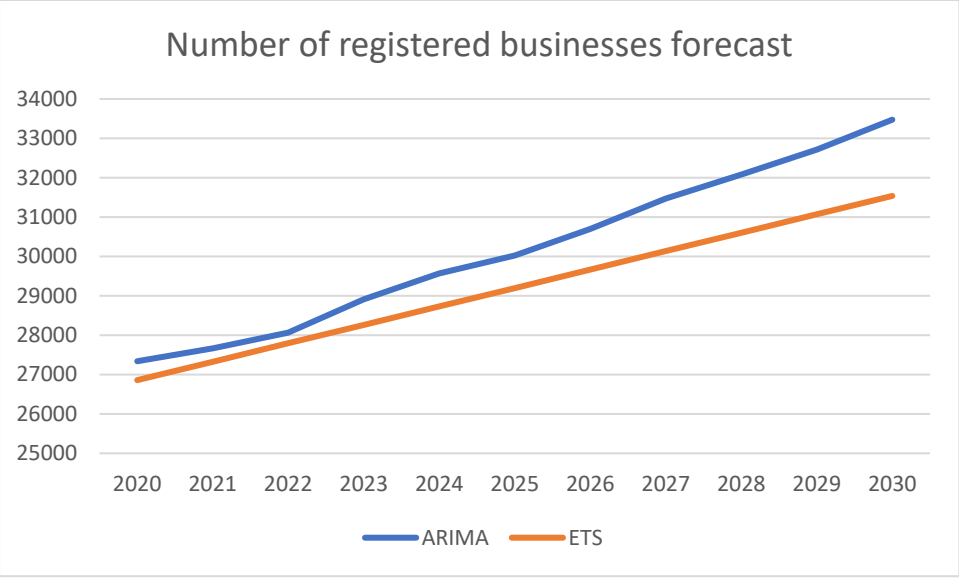
Year	Forecast	Lower Bound	Upper Bound
2020	27338	25316	29487
2021	27664	25236	30274
2022	28064	25589	30727
2023	28908	26127	31921
2024	29573	26333	33123
2025	30024	26627	33758
2026	30701	27128	34640
2027	31468	27565	35801
2028	32079	27919	36720
2029	32713	28364	37578
2030	33474	28869	38646

The forecast using Exponential Smoothing is presented as well for comparison between these two methods.



Year	Forecast	Lower Bound	Upper Bound
2020	26859	25253	28464
2021	27326	25671	28982
2022	27794	26090	29498
2023	28262	26510	30014
2024	28730	26932	30529
2025	29198	27353	31043

2026	29666	27776	31556
2027	30134	28199	32068
2028	30602	28623	32580
2029	31070	29048	33091
2030	31537	29473	33602

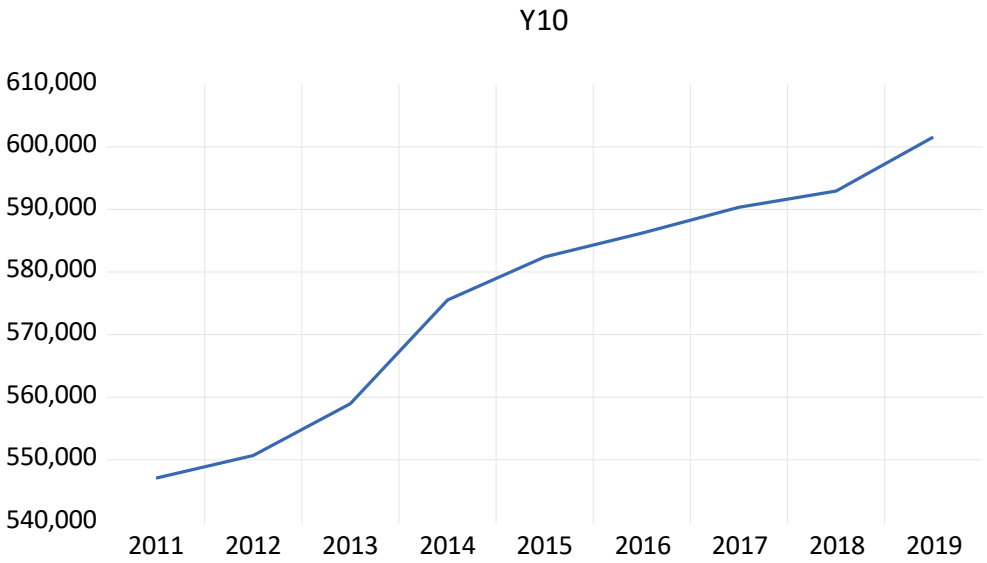


7.2.10 Modelling the number of the registered SMEs y10

The data is available from FSO only from year 2011 until year 2019. The next release of data is expected in November 2022. This could be a problem because of the very limited number of reads in this series.

Year	SMEs	Year	SMEs
2011	546,912	2016	586,054
2012	550,682	2017	590,253
2013	558,948	2018	592,915
2014	575,508	2019	601,392
2015	582,268		

The plot of the series shows non-stationarity, and so does the unit root test. Taking the first difference could make the series stationary.



Null Hypothesis: Y10 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=1)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-0.859382	0.7439
Test critical values:	1% level	-4.582648	
	5% level	-3.320969	
	10% level	-2.801384	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 8

The unit root test after taking first order difference is presented. But it does not make the series stationary.

Null Hypothesis: D(Y10) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=1)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-1.961168	0.2930
Test critical values:	1% level	-4.803492	
	5% level	-3.403313	
	10% level	-2.841819	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 7

The second difference is taken now. However, the series is still non-stationary

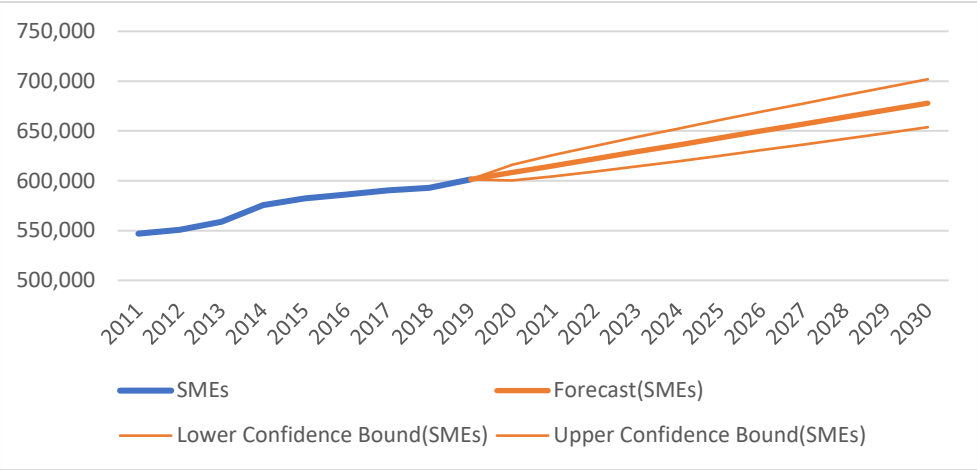
Null Hypothesis: D(Y10,2) has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=1)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.800197	0.1210
Test critical values:	1% level	-5.604618	
	5% level	-3.694851	
	10% level	-2.982813	

*MacKinnon (1996) one-sided p-values.
Warning: Probabilities and critical values calculated for 20 observations
and may not be accurate for a sample size of 5

It is not possible to continue with ARIMA method for this series. The number of entries is too little.

The Exponential Smoothing ETS is used for this series.



The number of SMEs will continue to increase which is great for the Swiss economy as it is majorly based on SMEs.

The results of the forecast are presented.

Year	Forecast	Lower Bound	Upper Bound
2020	608,248	600,318	616,178
2021	615,209	604,535	625,883
2022	622,171	609,322	635,020
2023	629,132	614,423	643,842
2024	636,094	619,730	652,457
2025	643,055	625,187	660,923
2026	650,016	630,758	669,275
2027	656,978	636,420	677,535
2028	663,939	642,157	685,721
2029	670,901	647,957	693,844
2030	677,862	653,810	701,914

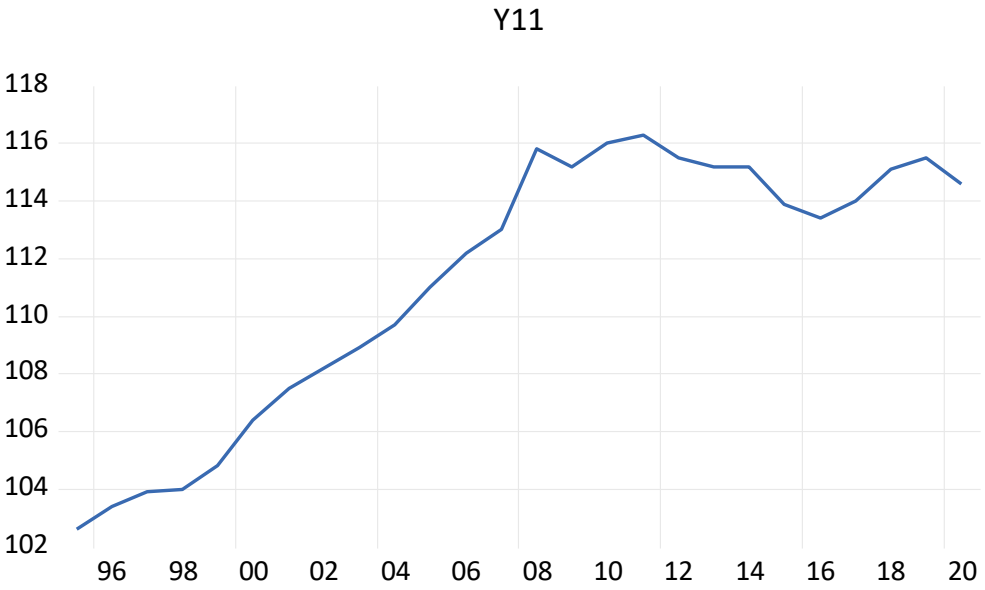
7.2.11 Modelling inflation y11

Data from year 1995 until 2020 is available from FSO with inflation in May 1993 is set to 100.

The data and the plot are both presented. The plot shows that the series is non-stationary.

Year	Inflation	Year	Inflation	Year	Inflation	Year	Inflation
1995	102.6	2002	108.20	2009	115.20	2016	113.40
1996	103.4	2003	108.90	2010	116.00	2017	114.00
1997	103.9	2004	109.70	2011	116.30	2018	115.10

1998	104	2005	111.00	2012	115.50	2019	115.50
1999	104.8	2006	112.20	2013	115.20	2020	114.60
2000	106.40	2007	113.00	2014	115.20		
2001	107.50	2008	115.80	2015	113.90		



The unit root test shows that the series is non-stationary.

Null Hypothesis: Y11 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.210909	0.2075
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

When taking the first difference, the series becomes stationary.

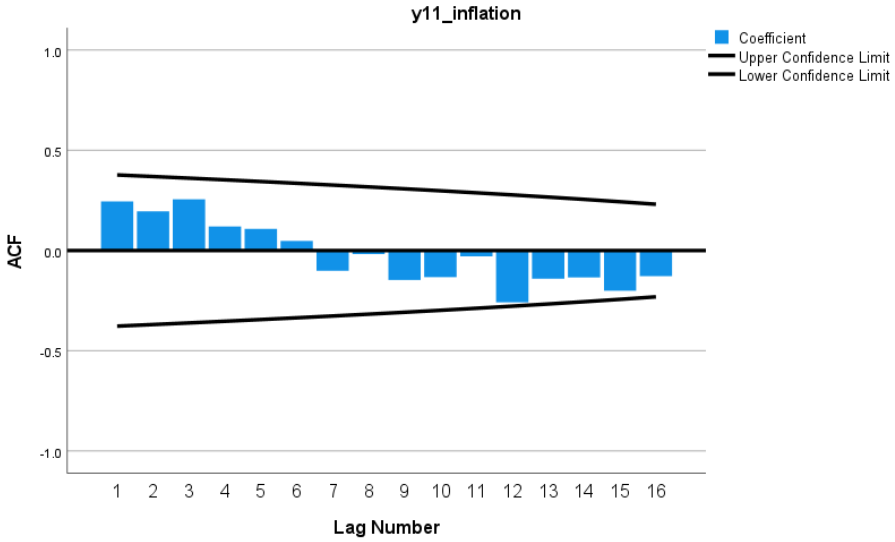
Null Hypothesis: D(Y11) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=5)

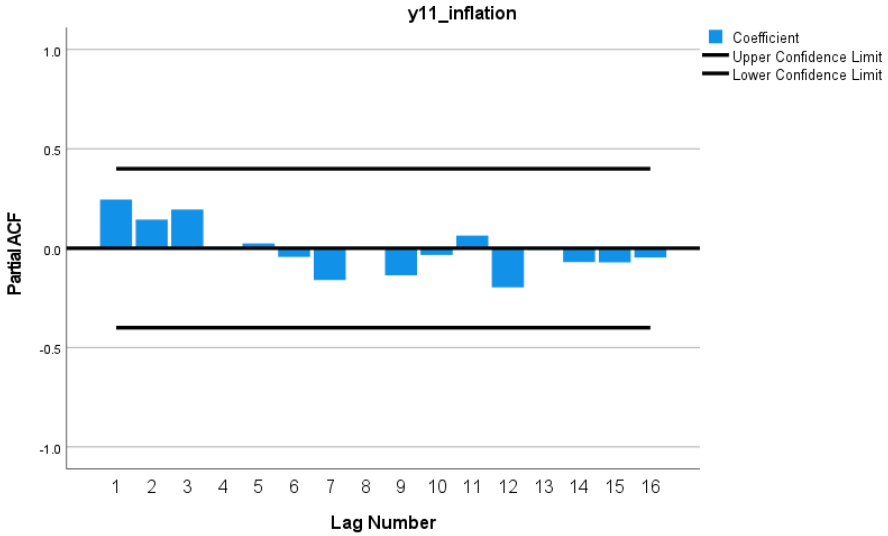
		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-3.422964	0.0201
Test critical values:	1% level	-3.737853	
	5% level	-2.991878	
	10% level	-2.635542	

*MacKinnon (1996) one-sided p-values.

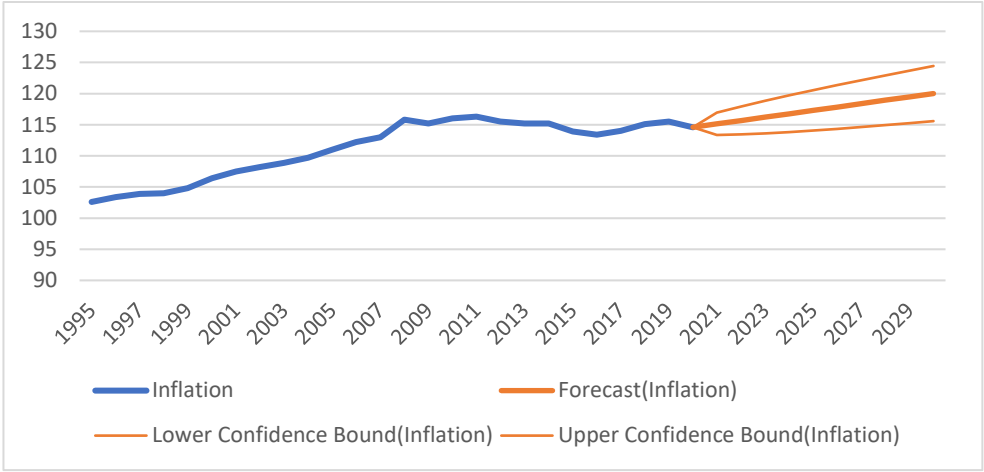
The correlogram for the PACF and ACF shows no significance. This means that the series is not suitable for ARIMA modelling. The graphic plot suggests also that this series is not ARIMA suitable.

Only Exponential Smoothing ETS is possible for this forecast.





The results of the forecast are presented.



The results suggest that the inflation will steadily increase in the coming decade but within accepted levels.

Year	Forecast	Lower Bound	Upper Bound
2021	115.1407521	113.35	116.93
2022	115.6815043	113.45	117.92
2023	116.2222564	113.61	118.83
2024	116.7630085	113.83	119.70
2025	117.3037607	114.07	120.53
2026	117.8445128	114.34	121.35
2027	118.385265	114.63	122.14

2028	118.9260171	114.94	122.92
2029	119.4667692	115.25	123.68
2030	120.0075214	115.58	124.43

7.2.12 Modelling activity rates y12

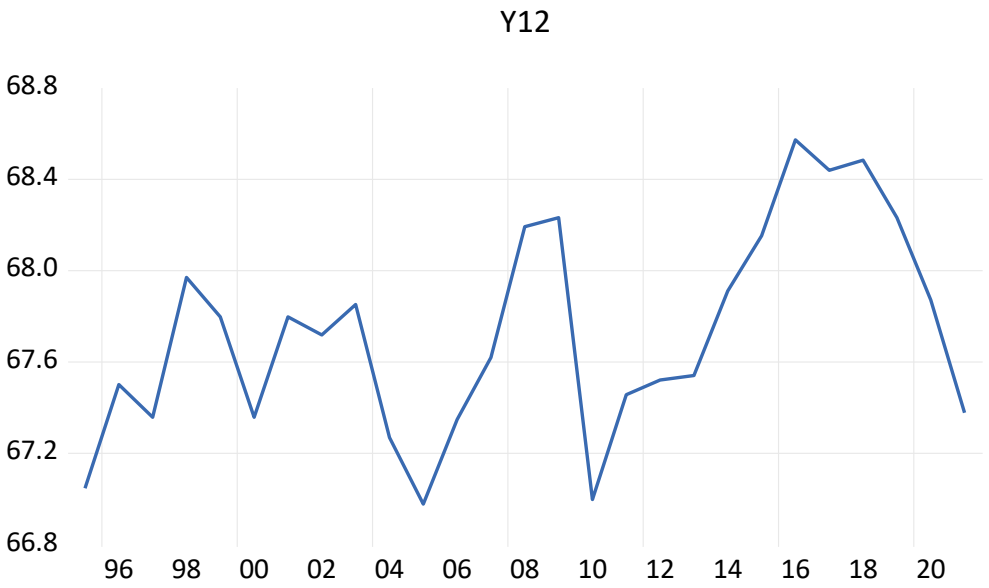
In the field of economically active population and the labor market participation, this variable presents the labor market participation rate in full-time equivalent.

The taken data is published by FSO. There is significant difference between male and female participation in the labor market. The data is presented but only the cumulative total figure will be analyzed. However, what is noticeable is that the women participation increased from 55.8% in 1995 to 62.2 in 2021. The participation of males dropped from 79% in 1995 to 72% in 2021.

Year	total	men	women	Year	total	men	women
1995	67.05	79.03	55.85	2009	68.23	75.24	61.56
1996	67.50	78.79	56.95	2010	67.00	74.34	59.98
1997	67.36	78.55	56.92	2011	67.46	74.69	60.54
1998	67.97	78.49	58.15	2012	67.52	74.50	60.84
1999	67.80	78.11	58.16	2013	67.54	74.19	61.14
2000	67.36	77.77	57.63	2014	67.91	74.14	61.90
2001	67.80	77.40	58.83	2015	68.15	74.22	62.28
2002	67.72	76.71	59.30	2016	68.57	74.50	62.84
2003	67.85	76.79	59.46	2017	68.44	74.47	62.61
2004	67.27	75.97	59.11	2018	68.48	74.24	62.91
2005	66.98	75.10	59.34	2019	68.23	73.65	62.98
2006	67.35	75.41	59.76	2020	67.87	73.39	62.51
2007	67.62	75.77	59.94	2021	67.38	72.68	62.23

As discussed, only the total figure is necessary to be forecasted using ARIMA method. It is not straight forward to decide from the graph if the series is stationary or not.

This will be decided by the unit root test.



The test suggests that the series is non-stationary.

Null Hypothesis: Y12 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.852415	0.0649
Test critical values:	1% level	-3.711457	
	5% level	-2.981038	
	10% level	-2.629906	

*MacKinnon (1996) one-sided p-values.

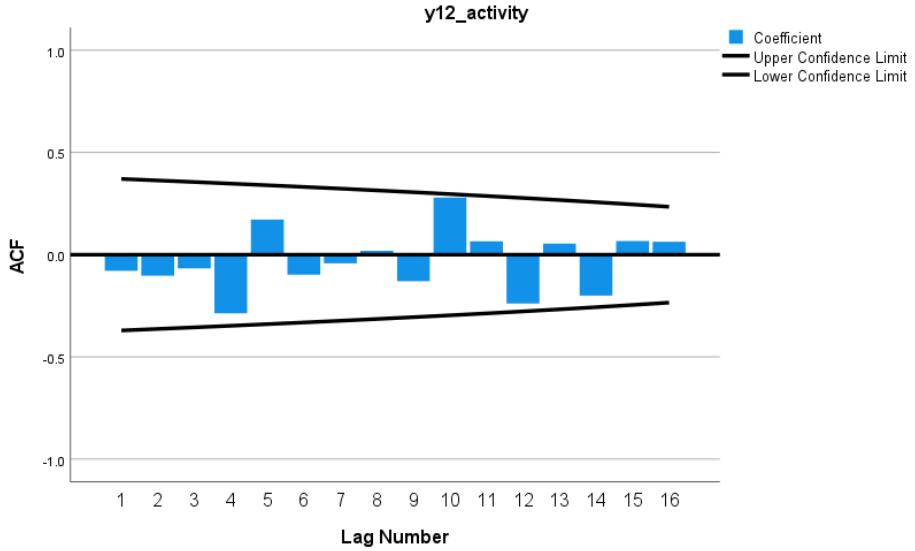
By taking the first difference it becomes stationary.

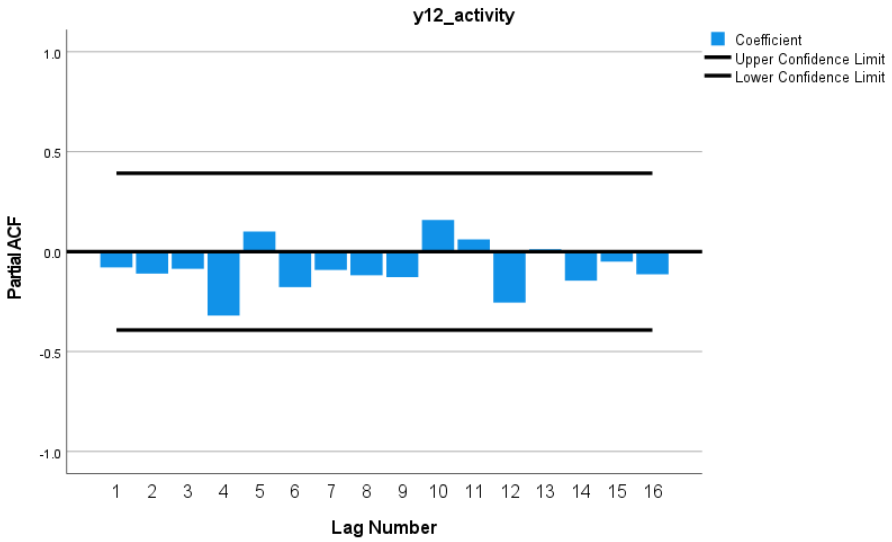
Null Hypothesis: D(Y12) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-5.158914	0.0003
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

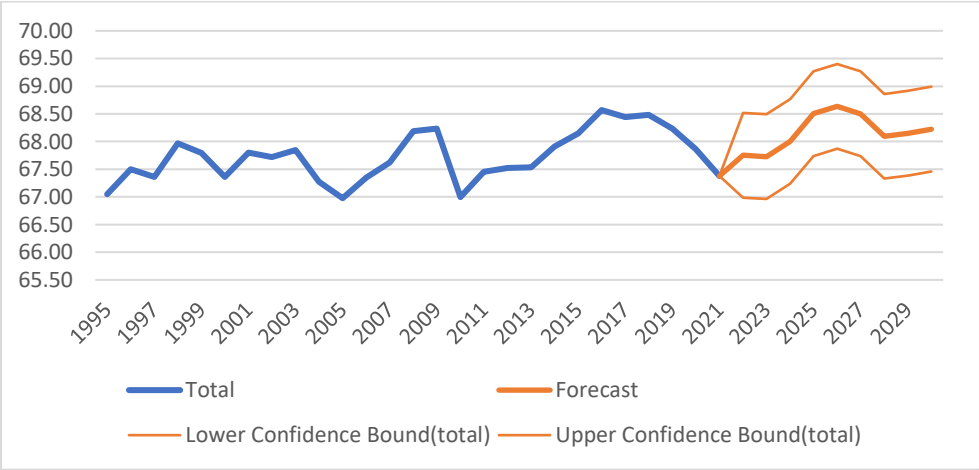
*MacKinnon (1996) one-sided p-values.

The correlogram analysis implies that this time series is not suitable for ARIMA forecasting. The series will be forecasted by the Exponential Smoothing ETS.





The results of the forecast are presented.

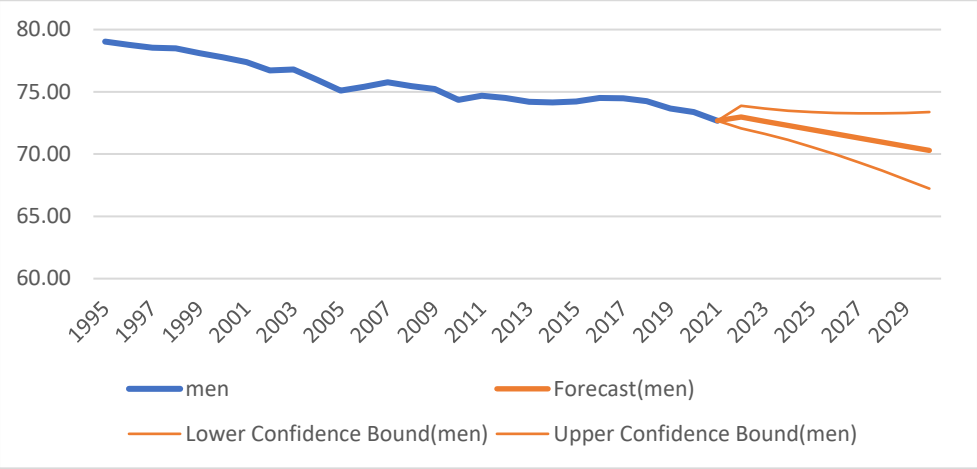


It is quite interesting to see that the Exponential Smoothing ETS forecast has captured what is similar to seasonality. However, it is not easy to explain this matter, but it could be an economy cycle where people tend to work more for few years and then work less in the proceeding years. Nevertheless, the variance is rather low which downplays such interpretation.

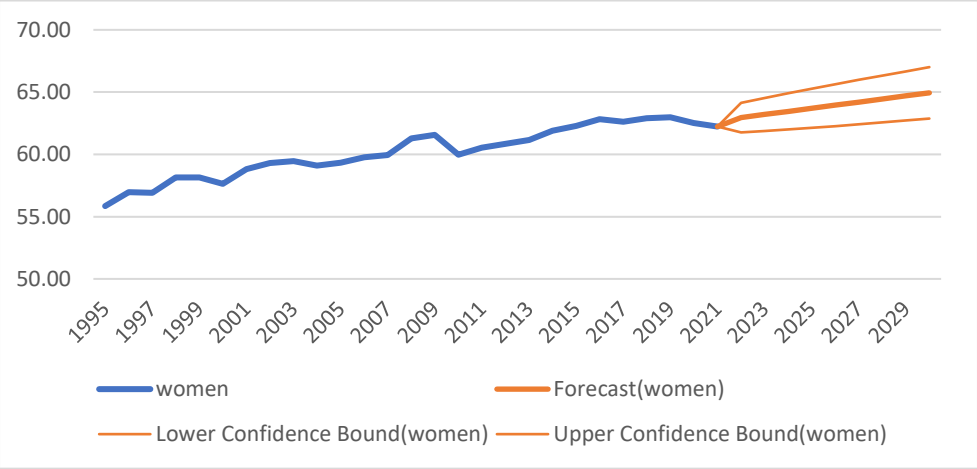
The forecasted values are presented.

Year	Forecast	Lower Bound	Upper Bound
2022	67.75	66.99	68.52
2023	67.73	66.96	68.49
2024	68.00	67.24	68.77
2025	68.50	67.74	69.27
2026	68.64	67.87	69.40
2027	68.50	67.74	69.27
2028	68.10	67.33	68.86
2029	68.15	67.39	68.91
2030	68.22	67.46	68.99

By making the forecast for men, the result suggests that men's participation in the economy will drop



While the participation of the women will increase.



Generally speaking, the forecast shows that no significant change will occur to the activity rate for the foreseeable future. In other words, it does not seem that people will be working less hours for the same or more income as being claimed by technology promotors and Smart Society promotors.

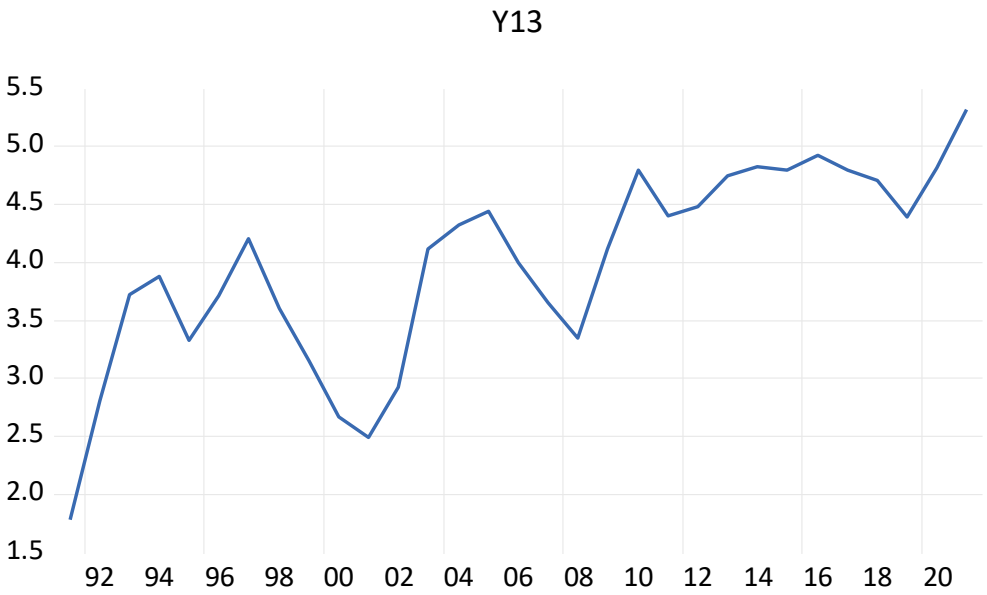
7.2.13 Modelling unemployment, variables y13, y14, y15, y16, y17

The table shows the forecast variables with their discerption. The data is published by the Worldbank.

Variable	Description
$y13$	Unemployment, total (% of total labor force)
$y14$	Unemployment, male (% of male labor force)
$y15$	Unemployment, female (% of female labor force)
$y16$	Unemployment with basic education (% of total labor force with basic education)
$y17$	Unemployment with advanced education (% of total labor force with advanced education)

	$y13$	$y14$	$y15$	$y16$	$y17$
Year	Total	Male	Female	Basic	Advanced
1991	1.78	1.22	2.52	2.23	1.23
1992	2.81	2.26	3.53	4.72	2.34
1993	3.72	3.07	4.57	5.46	2.26
1994	3.88	3.47	4.42	6.05	3.15
1995	3.33	2.88	3.92	6.58	2.12
1996	3.71	3.41	4.08		
1997	4.2	4.37	3.99		
1998	3.6	3.17	4.14	5.2	2.98
1999	3.15	2.81	3.57	5.48	1.85
2000	2.67	2.3	3.13	4.69	1.34
2001	2.49	1.7	3.46	4.84	1.46
2002	2.92	2.78	3.1	4.48	2.21
2003	4.12	3.81	4.49	6.51	2.99
2004	4.32	3.94	4.76	7.37	2.71
2005	4.44	3.89	5.09	7.82	2.8
2006	4	3.4	4.71	7.12	2.42
2007	3.65	2.93	4.51	6.88	2.19
2008	3.35	2.82	3.97	6.11	1.9
2009	4.12	3.77	4.52	7.48	2.74
2010	4.8	4.48	5.19	7.91	3.1
2011	4.4	4.07	4.79	7.92	2.96
2012	4.48	4.28	4.73	7.72	3.03
2013	4.75	4.6	4.92	8.28	3.37
2014	4.83	4.69	4.99	8.61	3.43
2015	4.8	4.7	4.91	8.72	3.52
2016	4.92	4.84	5.01	9.16	3.32
2017	4.8	4.57	5.06	8.17	3.74
2018	4.71	4.37	5.11	8.07	3.48
2019	4.39	4.11	4.71	7.98	3.25
2020	4.82	4.66	5	8.27	3.51
2021	5.321				

The start is with forecasting y13: Unemployment, total (% of total labor force) using ARIMA method. The plot shows that the series is non-stationary. The unit root test confirms this result.



Null Hypothesis: Y13 has a unit root
Exogenous: Constant
Lag Length: 1 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.125485	0.2367
Test critical values:	1% level	-3.679322	
	5% level	-2.967767	
	10% level	-2.622989	

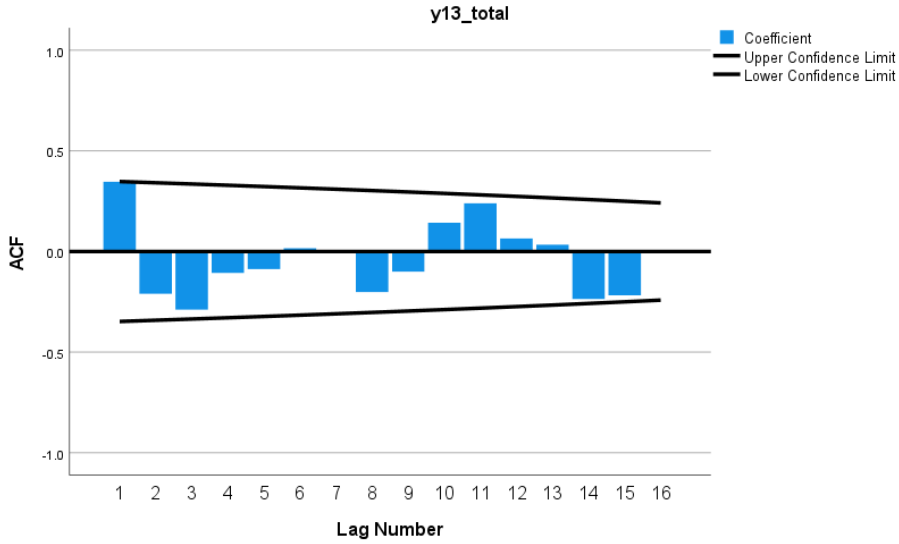
*MacKinnon (1996) one-sided p-values.

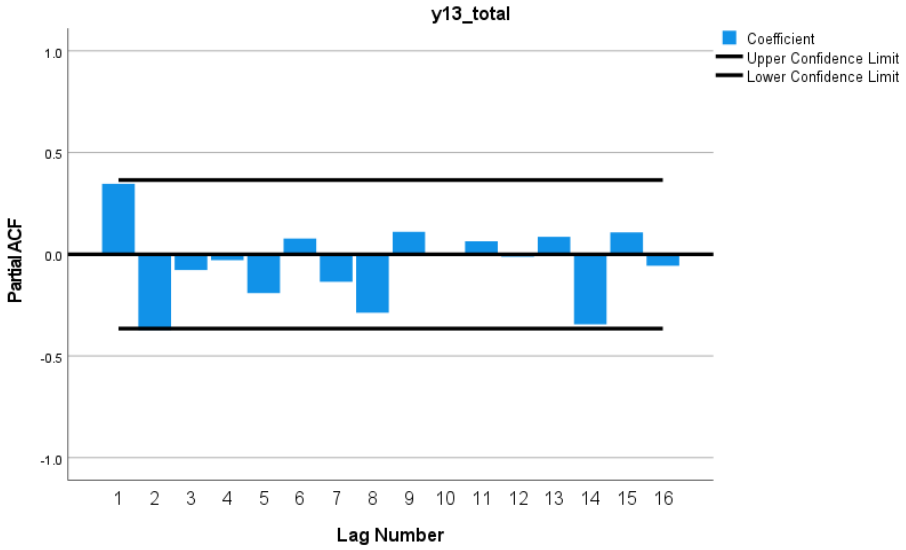
Taking the first order difference makes the series stationary. The analysis of the correlogram will follow.

Null Hypothesis: D(Y13) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.064439	0.0039
Test critical values:	1% level	-3.679322	
	5% level	-2.967767	
	10% level	-2.622989	

*MacKinnon (1996) one-sided p-values.





Despite that the drift does not occur at the first lag exactly for the PACF, the value 1 for the moving average (q parameter) is considered.

The correlogram of the ACF and PACF suggest the values: 1 for the p parameter, and 1 and 2 for the q parameter.

There are several ARIMA models to analyze and evaluate: ARIMA (1,1,0), ARIMA (1,1,1), ARIMA (1,1,2), ARIMA (0,1,1), and ARIMA (0,1,2).

The model ARIMA (1,1,0) is not a good model because the p-value for the constant is too high (bigger than 0.05). This makes the model insignificant.

Dependent Variable: D(LY13)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 10:37
Sample: 1992 2021
Included observations: 30
Convergence achieved after 17 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.049643	0.048401	1.025670	0.3141
AR(1)	0.463597	0.182112	2.545677	0.0169
SIGMASQ	0.018008	0.005348	3.367287	0.0023

R-squared	0.168246	Mean dependent var	0.036502
Adjusted R-squared	0.106635	S.D. dependent var	0.149659
S.E. of regression	0.141455	Akaike info criterion	-0.970969
Sum squared resid	0.540255	Schwarz criterion	-0.830849
Log likelihood	17.56454	Hannan-Quinn criter.	-0.926144
F-statistic	2.730764	Durbin-Watson stat	1.615462
Prob(F-statistic)	0.083163		

Inverted AR Roots	.46

The model ARIMA (1,1,1) is also not suitable for the same reason (too high p-value for several parameters). This also suggests that ARIMA (1,1,2) is a bad model as well, but this will be tested.

Dependent Variable: D(LY13)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 10:39
Sample: 1992 2021
Included observations: 30
Convergence achieved after 28 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.044623	0.044520	1.002319	0.3254
AR(1)	0.155961	0.338980	0.460090	0.6493
MA(1)	0.464989	0.323392	1.437851	0.1624
SIGMASQ	0.016227	0.005150	3.150630	0.0041

R-squared	0.250522	Mean dependent var	0.036502
Adjusted R-squared	0.164043	S.D. dependent var	0.149659
S.E. of regression	0.136834	Akaike info criterion	-1.002918
Sum squared resid	0.486814	Schwarz criterion	-0.816092
Log likelihood	19.04377	Hannan-Quinn criter.	-0.943151
F-statistic	2.896930	Durbin-Watson stat	1.909885
Prob(F-statistic)	0.054158		

Inverted AR Roots	.16	
Inverted MA Roots	-.46	

ARIMA (1,1,2) is a bad model as expected from the previous result.

Dependent Variable: D(LY13)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 10:42
Sample: 1992 2021
Included observations: 30
Convergence achieved after 26 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.035204	0.031940	1.102190	0.2805
AR(1)	0.457984	0.218473	2.096291	0.0459
MA(2)	-0.401906	0.223492	-1.798304	0.0838
SIGMASQ	0.016203	0.004586	3.533102	0.0016

R-squared	0.251637	Mean dependent var	0.036502
Adjusted R-squared	0.165287	S.D. dependent var	0.149659
S.E. of regression	0.136732	Akaike info criterion	-1.004296
Sum squared resid	0.486089	Schwarz criterion	-0.817469
Log likelihood	19.06443	Hannan-Quinn criter.	-0.944528
F-statistic	2.914164	Durbin-Watson stat	1.721857
Prob(F-statistic)	0.053212		

Inverted AR Roots	.46	
Inverted MA Roots	.63	-.63

The moving average models have proved to be not applicable through out all these economic parameters that are selected for the forecast. The test will follow either way to confirm or deny this argument.

ARIMA (0,1,1) is not a good model as the p-value for the constant is too high.

Dependent Variable: D(LY13)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 10:44
Sample: 1992 2021
Included observations: 30
Convergence achieved after 35 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.042211	0.041085	1.027404	0.3133
MA(1)	0.548648	0.193482	2.835657	0.0086
SIGMASQ	0.016402	0.004957	3.309210	0.0027

R-squared	0.242424	Mean dependent var	0.036502
Adjusted R-squared	0.186307	S.D. dependent var	0.149659
S.E. of regression	0.135000	Akaike info criterion	-1.060510
Sum squared resid	0.492074	Schwarz criterion	-0.920390
Log likelihood	18.90765	Hannan-Quinn criter.	-1.015684
F-statistic	4.319992	Durbin-Watson stat	1.799837
Prob(F-statistic)	0.023564		

Inverted MA Roots	-.55

Surprisingly, ARIMA (0,1,2) is possible good model for this time series.

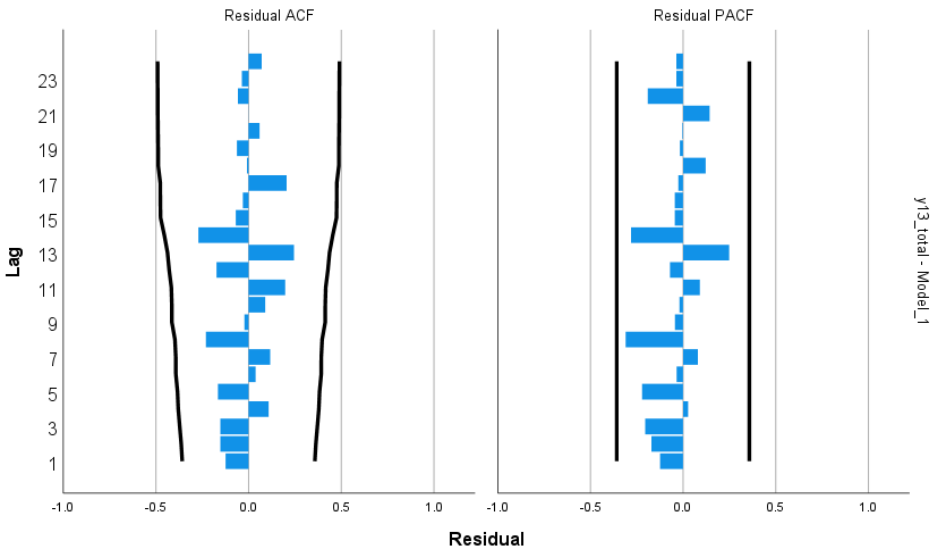
Dependent Variable: D(LY13)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 10:45
Sample: 1992 2021
Included observations: 30
Convergence achieved after 20 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.022235	0.009790	2.271073	0.0313
MA(2)	-0.783776	0.250099	-3.133859	0.0041
SIGMASQ	0.016853	0.005132	3.284123	0.0028

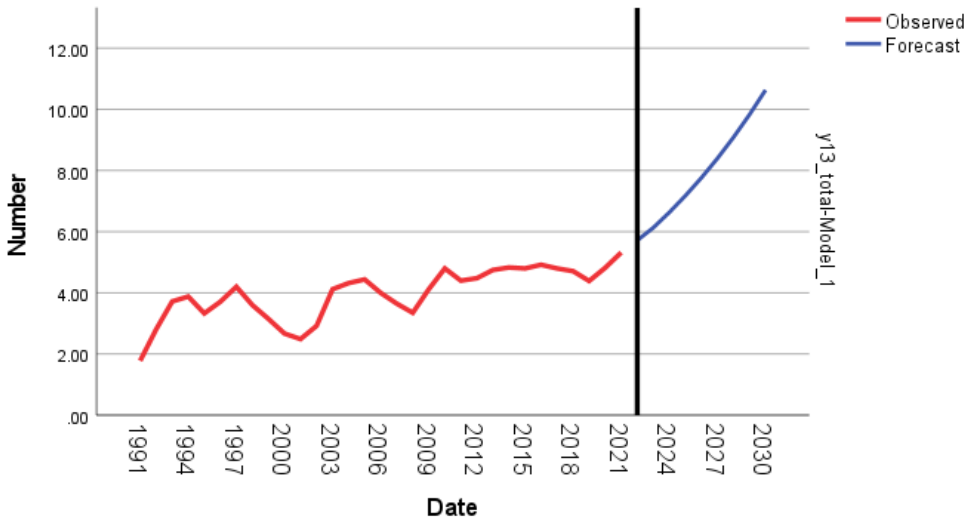
R-squared	0.221627	Mean dependent var	0.036502
Adjusted R-squared	0.163970	S.D. dependent var	0.149659
S.E. of regression	0.136840	Akaike info criterion	-0.981879
Sum squared resid	0.505582	Schwarz criterion	-0.841759
Log likelihood	17.72819	Hannan-Quinn criter.	-0.937054
F-statistic	3.843871	Durbin-Watson stat	1.357136
Prob(F-statistic)	0.033965		

Inverted MA Roots	.89	-.89

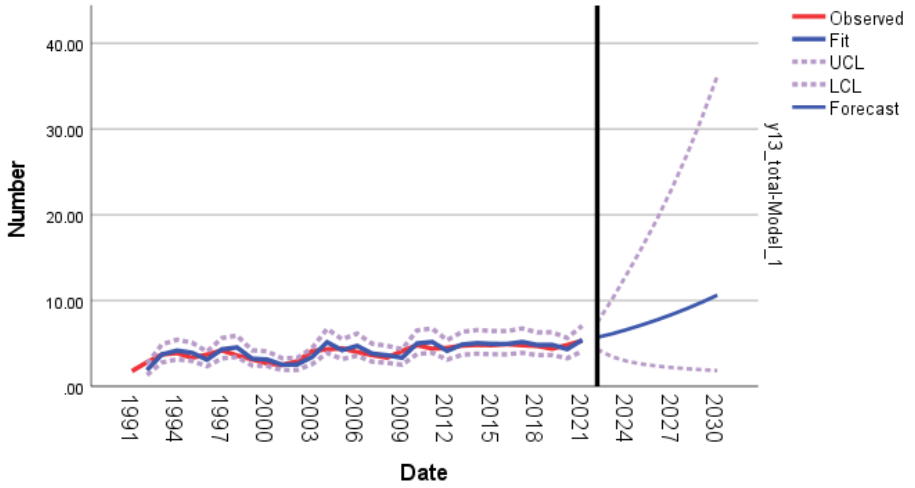
The residual correlogram shows white noise.



The forecast of ARIMA (0,1,2) is presented.



The forecast suggests that y13 will increase exponentially over the next decade. But this outcome should be looked at very critically. First, the moving average method is not expected to be suitable for the entire forecast as has proved so far. Second, the adjusted r-squared value of the model is very low (0.18). Third, the visual analysis in time series is not less important than the statistical analysis. The forecasted line does not correspond to the trend of the previous values in the forecast graph. Finally, the values of the upper bond say that the unemployment could reach extreme high level by 2030 (36%) , and this finding makes no sense.



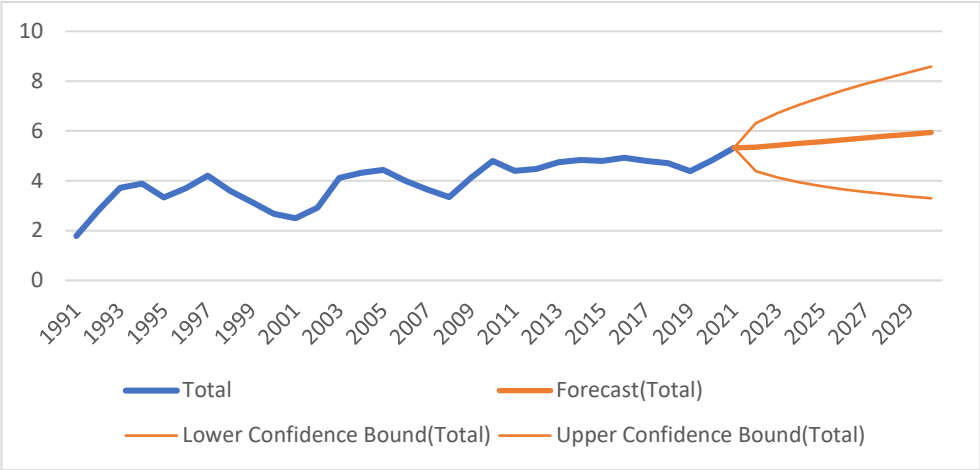
Just because a variable is possible to be forecasted using ARIMA, it does not mean necessarily that ARIMA is the correct method for this variable.

The values of the forecast with the upper and lower bounds are presented.

Year	Forecast	Lower Bound	Upper Bound
2022	5.72	4.31	7.44
2023	6.13	3.45	10.17
2024	6.63	2.92	13.17
2025	7.18	2.59	16.25
2026	7.76	2.36	19.55
2027	8.40	2.19	23.15
2028	9.09	2.05	27.09
2029	9.83	1.94	31.42
2030	10.63	1.85	36.20

This time series will be forecasted using the Exponential Smoothing ETS. The forecast presents more logical predictions than the ARIMA (0,1,2).

The values of the forecast with their upper and lower bound are presented.



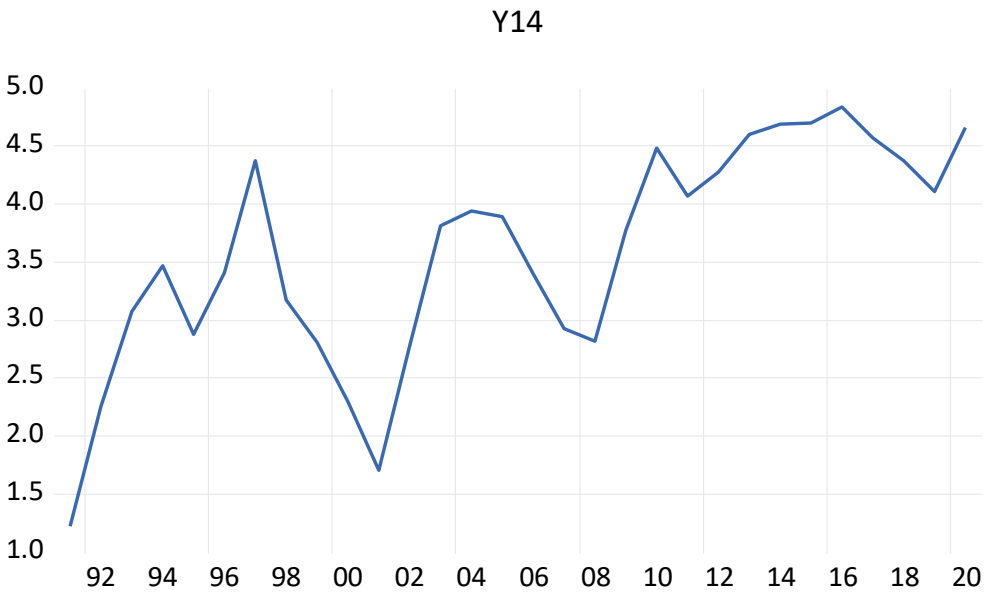
Year	Forecast	Upper Bound	Lower Bound
2022	5.35	4.39	6.31
2023	5.42	4.13	6.72
2024	5.50	3.94	7.06
2025	5.57	3.79	7.36
2026	5.64	3.66	7.63
2027	5.72	3.55	7.89
2028	5.79	3.46	8.13
2029	5.87	3.37	8.36
2030	5.94	3.30	8.58

The Exponential Smoothing ETS is clearly more realistic and representative of unemployment variables specially in comparison to the second order of the moving average component of ARIMA.

For the remainder of the unemployment variables, the second order moving average ARIMA model will not be considered.

7.2.14 Modelling unemployment, male (% of male labor force) y14

The plot and the unit root test suggest that the series is non-stationary.



Null Hypothesis: Y14 has a unit root
Exogenous: Constant
Lag Length: 4 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-1.193040	0.6610
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

*MacKinnon (1996) one-sided p-values.

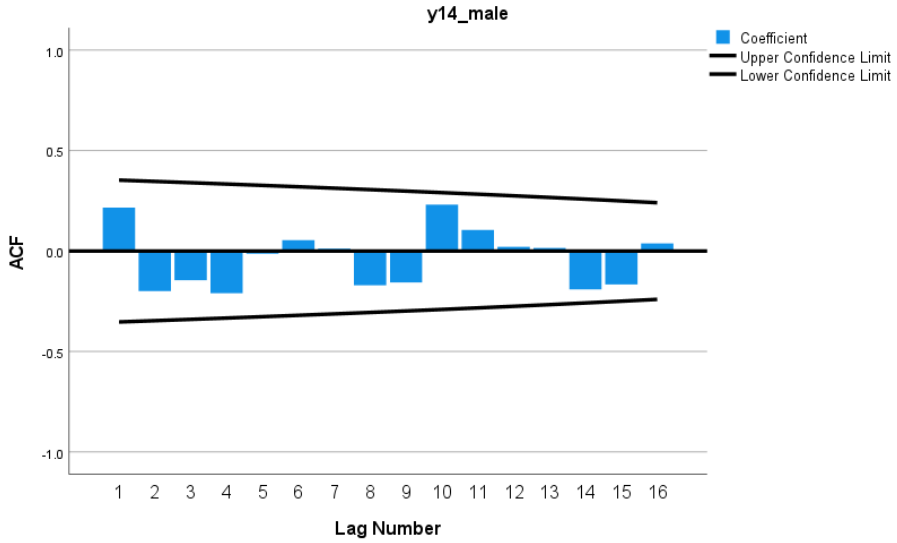
After taking the first order difference, the series become stationary.

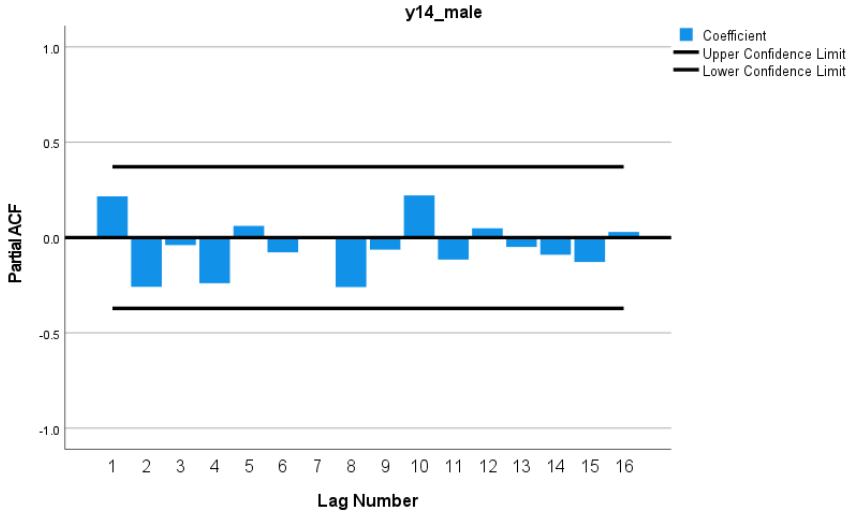
Null Hypothesis: D(Y14) has a unit root
Exogenous: Constant
Lag Length: 3 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-4.007934	0.0052
Test critical values:	1% level	-3.724070	
	5% level	-2.986225	
	10% level	-2.632604	

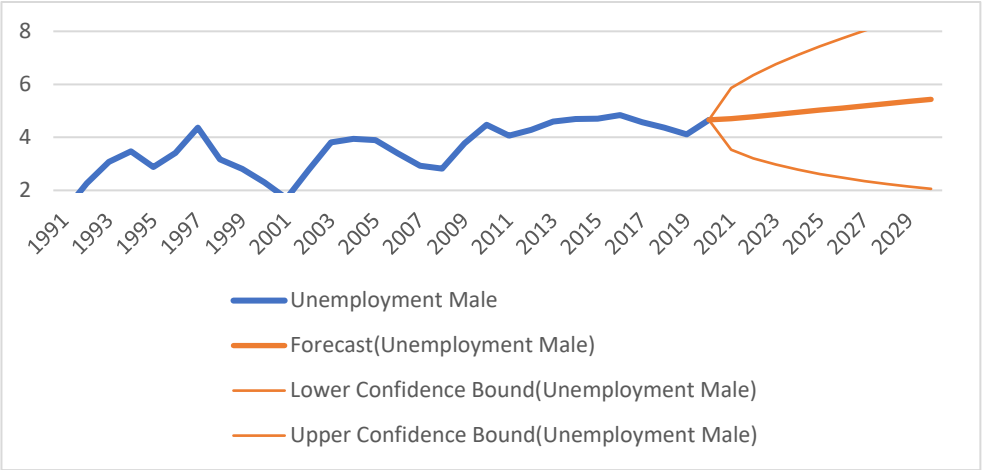
*MacKinnon (1996) one-sided p-values.

The correlogram of the correlation functions shows no significance. This means that ARIMA method is not suitable for this time series. In other words, the series is neither an autocorrelation process, nor a moving average process. Forecast will be made using the Exponential Smoothing ETS.





The result of the forecast is presented.



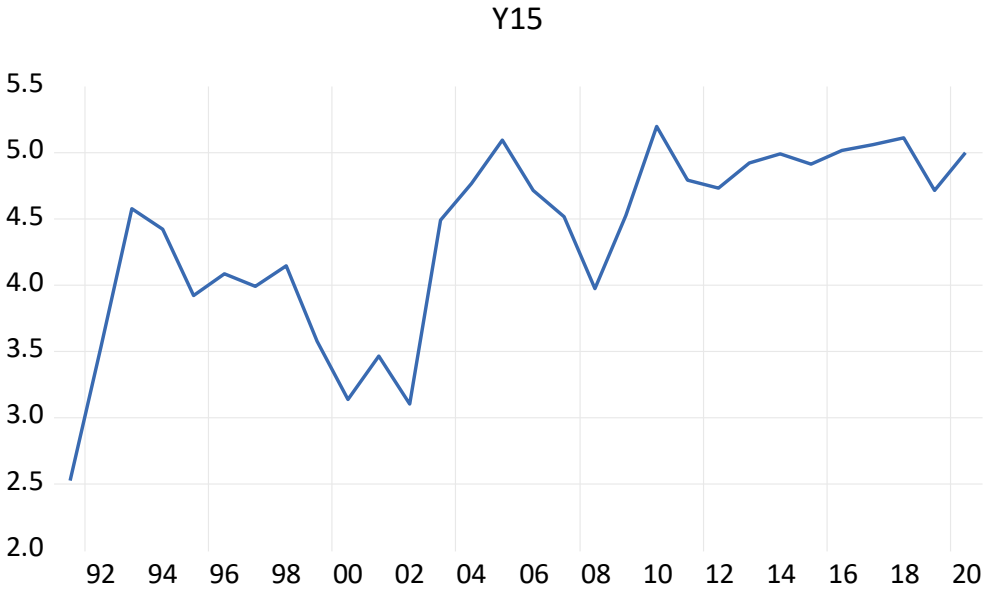
The unemployment rates will increase slightly for the next decade but will remain below 6%. The values of the forecast are presented.

Year	Forecast	Upper Bound	Lower Bound
2021	4.70	3.53	5.87
2022	4.78	3.21	6.35
2023	4.86	2.97	6.75
2024	4.94	2.78	7.11
2025	5.03	2.62	7.43
2026	5.11	2.48	7.74
2027	5.19	2.35	8.02

2028	5.27	2.25	8.30
2029	5.35	2.15	8.56
2030	5.43	2.06	8.81

7.2.15 Modelling unemployment, female (% of female labor force) y15

The graph does not give a clear answer on whether or not the series is stationary. But the unit root test say it is stationary.

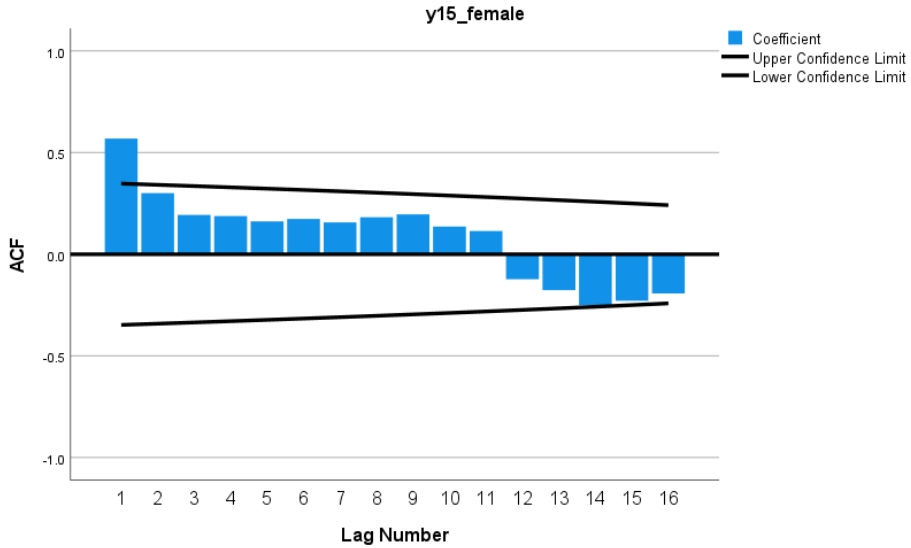


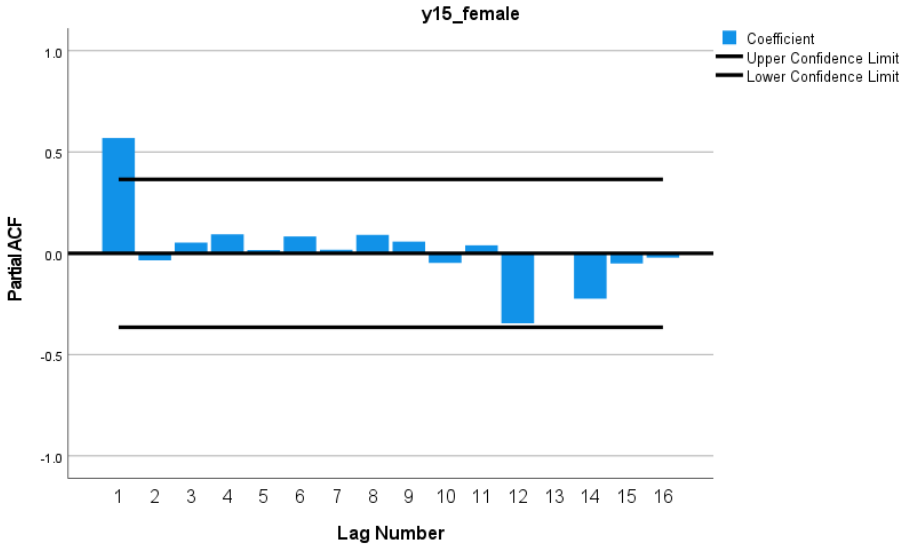
Null Hypothesis: Y15 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=7)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-3.091972	0.0383
Test critical values:	1% level	-3.679322	
	5% level	-2.967767	
	10% level	-2.622989	

*MacKinnon (1996) one-sided p-values.

The correlogram gives the possibility of value 1 for both of the ARIMA remaining parameters. Hence, D=0.





The followings are possible ARIMA models: ARIMA (1,0,0), ARIMA (0,0,1), and ARIMA (1,0,1).

ARIMA (1,0,0) is a possible suitable model.

Dependent Variable: LY15
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 11:42
Sample: 1991 2020
Included observations: 30
Convergence achieved after 76 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.418329	0.144525	9.813709	0.0000
AR(1)	0.800974	0.135208	5.924032	0.0000
SIGMASQ	0.015730	0.003980	3.952477	0.0005

R-squared	0.488070	Mean dependent var	1.458971
Adjusted R-squared	0.450149	S.D. dependent var	0.178289
S.E. of regression	0.132205	Akaike info criterion	-1.080088
Sum squared resid	0.471910	Schwarz criterion	-0.939968
Log likelihood	19.20132	Hannan-Quinn criter.	-1.035263
F-statistic	12.87077	Durbin-Watson stat	1.913103
Prob(F-statistic)	0.000119		

Inverted AR Roots	.80

ARIMA (0,0,1) is also a potential good model.

Dependent Variable: LY15
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 11:43
Sample: 1991 2020
Included observations: 30
Convergence achieved after 21 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.453556	0.058936	24.66324	0.0000
MA(1)	0.616138	0.199993	3.080793	0.0047
SIGMASQ	0.019654	0.005584	3.519511	0.0016

R-squared	0.360384	Mean dependent var	1.458971
Adjusted R-squared	0.313005	S.D. dependent var	0.178289
S.E. of regression	0.147775	Akaike info criterion	-0.875694
Sum squared resid	0.589613	Schwarz criterion	-0.735575
Log likelihood	16.13542	Hannan-Quinn criter.	-0.830869
F-statistic	7.606422	Durbin-Watson stat	1.461551
Prob(F-statistic)	0.002398		

Inverted MA Roots	-.62

However, ARIMA (1,0,1) is not a good model because the p-value for the moving average component is higher than 0.05.

Dependent Variable: LY15
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 11:43
Sample: 1991 2020
Included observations: 30
Convergence achieved after 65 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.425939	0.129806	10.98512	0.0000
AR(1)	0.720727	0.192871	3.736827	0.0009
MA(1)	0.203367	0.236376	0.860355	0.3975
SIGMASQ	0.015295	0.003817	4.007343	0.0005

R-squared	0.502247	Mean dependent var	1.458971
Adjusted R-squared	0.444813	S.D. dependent var	0.178289
S.E. of regression	0.132845	Akaike info criterion	-1.040751
Sum squared resid	0.458841	Schwarz criterion	-0.853925
Log likelihood	19.61127	Hannan-Quinn criter.	-0.980984
F-statistic	8.744899	Durbin-Watson stat	2.165072
Prob(F-statistic)	0.000353		

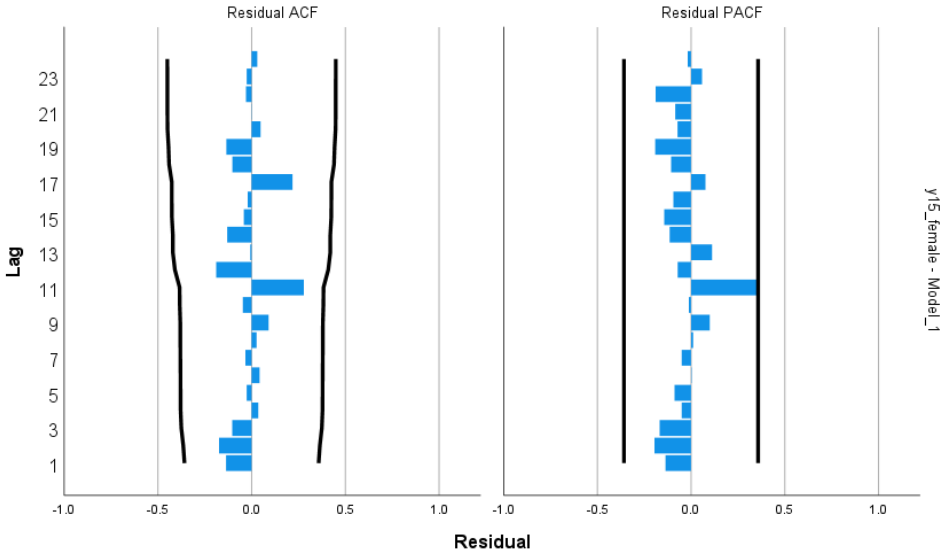
Inverted AR Roots	.72
Inverted MA Roots	-.20

The task now is to choose between the two models, ARIMA (1,0,0) also named ARMA (1,0) and ARIMA (0,0,1) aka ARMA (0,1).

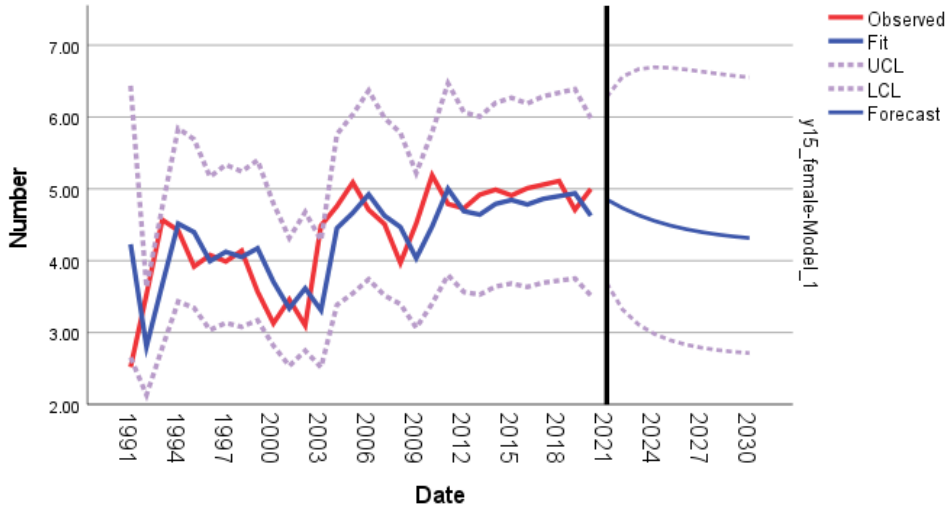
ARIMA (1,0,0) has a higher R-squared value, so it is more representative for this time series.

$y15$ will be forecasted using ARIMA (1,0,0). The outcomes of the forecast are presented.

The residual correlogram shows white noise.



The forecast predicts that the unemployment amongst women will decrease for the coming decade. Despite that the model seems like a good fit, this prediction should not be read separately from the forecast of the total unemployment ($y13$). These variables have very similar nature and are similarly affected by economy situation.

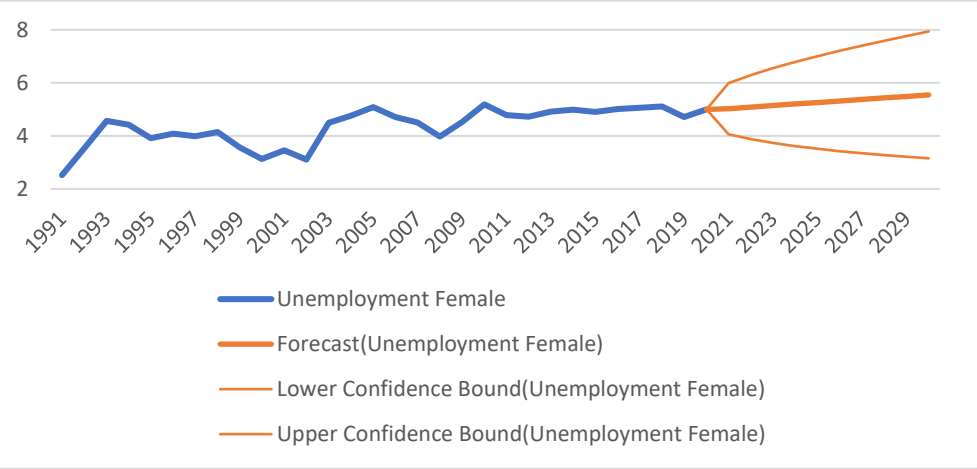


The values of the forecast are presented.

Year	Forecast	Lower Bound	Upper Bound
2021	4.85	3.69	6.28
2022	4.73	3.32	6.56
2023	4.64	3.11	6.67
2024	4.56	2.98	6.69
2025	4.49	2.89	6.69
2026	4.44	2.83	6.66
2027	4.40	2.79	6.63

2028	4.36	2.76	6.60
2029	4.34	2.73	6.58
2030	4.32	2.71	6.55

The Exponential Smoothing ETS is used now for this time series.

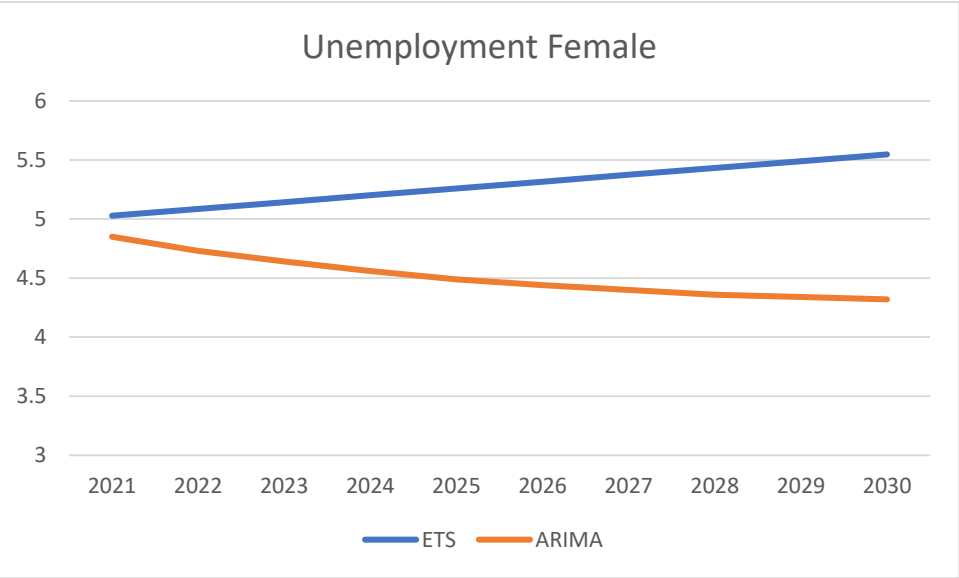


Now there is a contradict between the two forecasting methods in terms of the direction of movement.

The values of the forecast are presented.

Year	Forecast	Lower Bound	Upper Bound
2021	5.03	4.06	6.00
2022	5.09	3.88	6.30
2023	5.14	3.73	6.55
2024	5.20	3.61	6.79
2025	5.26	3.51	7.01
2026	5.32	3.42	7.21
2027	5.37	3.34	7.40
2028	5.43	3.27	7.59
2029	5.49	3.21	7.77
2030	5.55	3.15	7.94

The comparison between the two methods in order to select the most suitable one for this variable is very difficult.

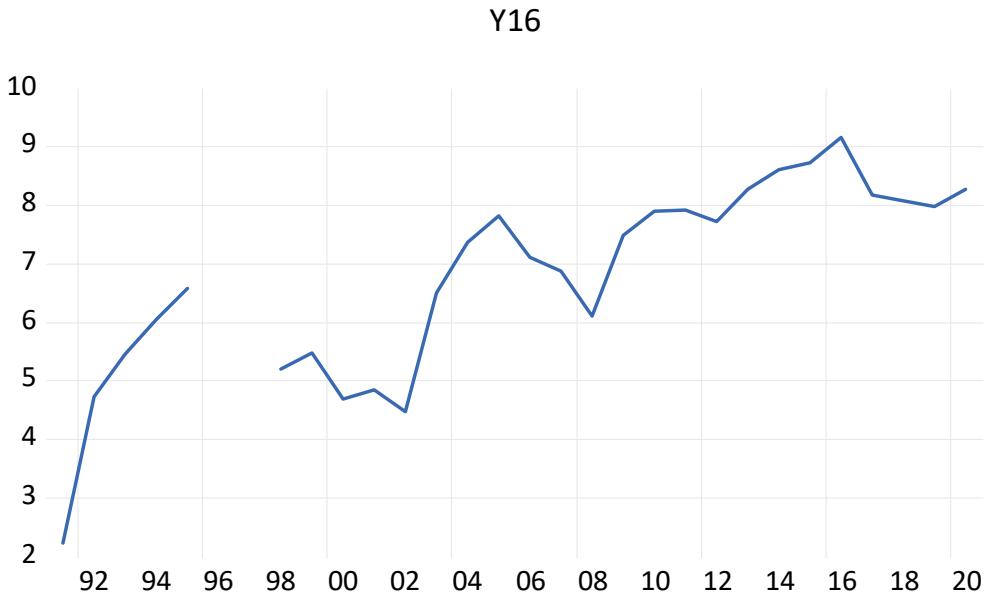


Nevertheless, the difference in forecast between the two methods will be only slightly over 1% in 10-year time. Despite the solidity of ARIMA method for this forecast, the Exponential Smoothing ETS gives result that are in concordance with the other unemployment variables. Therefore, the ETS appears to be more realistic, and the unemployment level amongst females will slightly increase.

7.2.16 Modelling unemployment with basic education y16

Variable $y16$ represents the unemployment with basic education (as % of total labor force with basic education). This segment of unemployment is particularly important to analyze because it is necessary to see how the IT dependent society will reflect on the level of education in terms of employment.

The graph shows that the series in stationary. The unit root test has the same result.

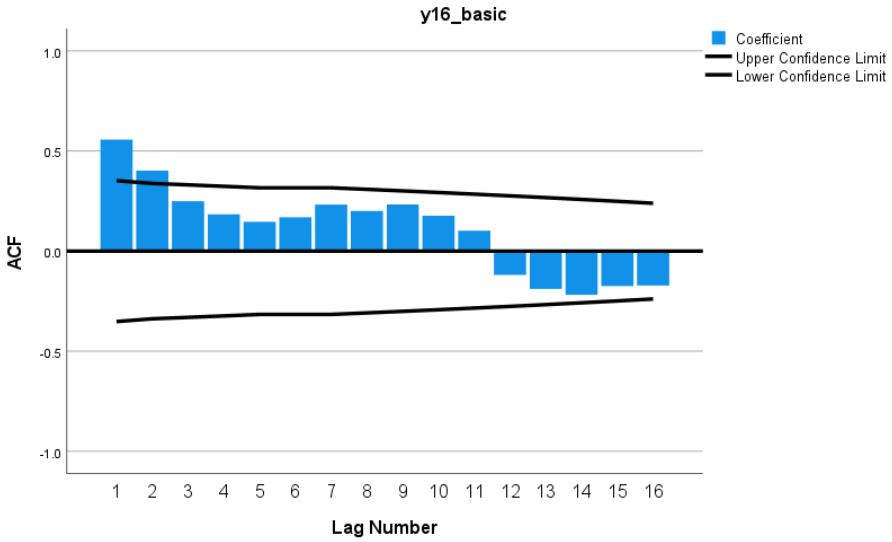


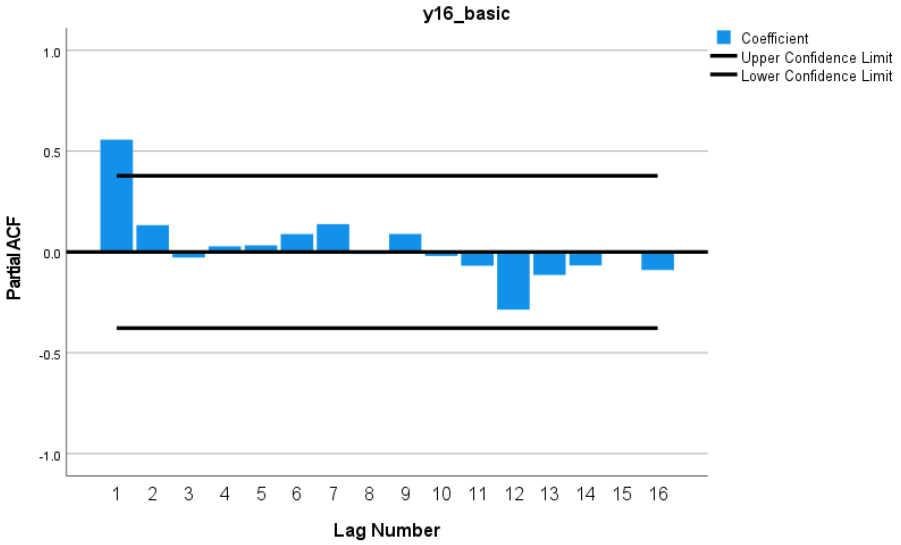
Null Hypothesis: Y16 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-3.386167	0.0210
Test critical values:	1% level	-3.711457	
	5% level	-2.981038	
	10% level	-2.629906	

*MacKinnon (1996) one-sided p-values.

The analysis of the correlogram suggests that the parameter p can be either 1 or 2, and the parameter q can be 1. (in addition to the 0 values for both parameters).





Consequently, the possible ARIMA models are: ARIMA (1,0,0), ARIMA (2,0,0), ARIMA (1,0,1), ARIMA (2,0,1), and ARIMA (0,0,1).

ARIMA (1,0,0) is a possible model

Dependent Variable: LY16
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:11
Sample: 1991 2020
Included observations: 28
Convergence achieved after 138 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.691498	0.488227	3.464576	0.0019
AR(1)	0.919388	0.112810	8.149894	0.0000
SIGMASQ	0.033050	0.007542	4.381903	0.0002

R-squared	0.618511	Mean dependent var	1.876963
Adjusted R-squared	0.587992	S.D. dependent var	0.299738
S.E. of regression	0.192395	Akaike info criterion	-0.257358
Sum squared resid	0.925398	Schwarz criterion	-0.114622
Log likelihood	6.603012	Hannan-Quinn criter.	-0.213722
F-statistic	20.26636	Durbin-Watson stat	2.142082
Prob(F-statistic)	0.000006		

Inverted AR Roots	.92

ARIMA (2,0,0) is a possible model as well

Dependent Variable: LY16
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:11
Sample: 1991 2020
Included observations: 28
Convergence achieved after 148 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.805383	0.206401	8.746957	0.0000
AR(2)	0.738439	0.111873	6.600663	0.0000
SIGMASQ	0.053986	0.012193	4.427455	0.0002

R-squared	0.376850	Mean dependent var	1.876963
Adjusted R-squared	0.326997	S.D. dependent var	0.299738
S.E. of regression	0.245895	Akaike info criterion	0.220514
Sum squared resid	1.511611	Schwarz criterion	0.363250
Log likelihood	-0.087190	Hannan-Quinn criter.	0.264149
F-statistic	7.559360	Durbin-Watson stat	1.020638
Prob(F-statistic)	0.002707		

Inverted AR Roots	.86	-.86

ARIMA (1,0,1) is not a good model as the p-value for the moving average component is higher than 0.05.

Dependent Variable: LY16
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:12
Sample: 1991 2020
Included observations: 28
Convergence achieved after 115 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.691562	0.484672	3.490115	0.0019
AR(1)	0.898443	0.136897	6.562918	0.0000
MA(1)	0.180869	0.492655	0.367131	0.7167
SIGMASQ	0.031969	0.006985	4.576928	0.0001

R-squared	0.630989	Mean dependent var	1.876963
Adjusted R-squared	0.584862	S.D. dependent var	0.299738
S.E. of regression	0.193125	Akaike info criterion	-0.207389
Sum squared resid	0.895131	Schwarz criterion	-0.017074
Log likelihood	6.903446	Hannan-Quinn criter.	-0.149208
F-statistic	13.67956	Durbin-Watson stat	2.494251
Prob(F-statistic)	0.000021		

Inverted AR Roots	.90	
Inverted MA Roots	-.18	

ARIMA (2,0,1) is not a good model either for the same reason.

Dependent Variable: LY16
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:13
Sample: 1991 2020
Included observations: 28
Failure to improve objective (non-zero gradients) after 86 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.678045	0.532042	3.153973	0.0043
AR(2)	0.860275	0.219361	3.921727	0.0006
MA(1)	1.000000	2651.976	0.000377	0.9997
SIGMASQ	0.031562	1.861427	0.016956	0.9866

R-squared	0.635691	Mean dependent var	1.876963
Adjusted R-squared	0.590153	S.D. dependent var	0.299738
S.E. of regression	0.191890	Akaike info criterion	-0.198106
Sum squared resid	0.883723	Schwarz criterion	-0.007791
Log likelihood	6.773484	Hannan-Quinn criter.	-0.139925
F-statistic	13.95941	Durbin-Watson stat	2.215041
Prob(F-statistic)	0.000018		

Inverted AR Roots	.93	-.93
Inverted MA Roots	-1.00	

ARIMA (0,0,1) is possible model for this time series.

Dependent Variable: LY16
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:14
Sample: 1991 2020
Included observations: 28
Convergence achieved after 10 iterations
Coefficient covariance computed using outer product of gradients

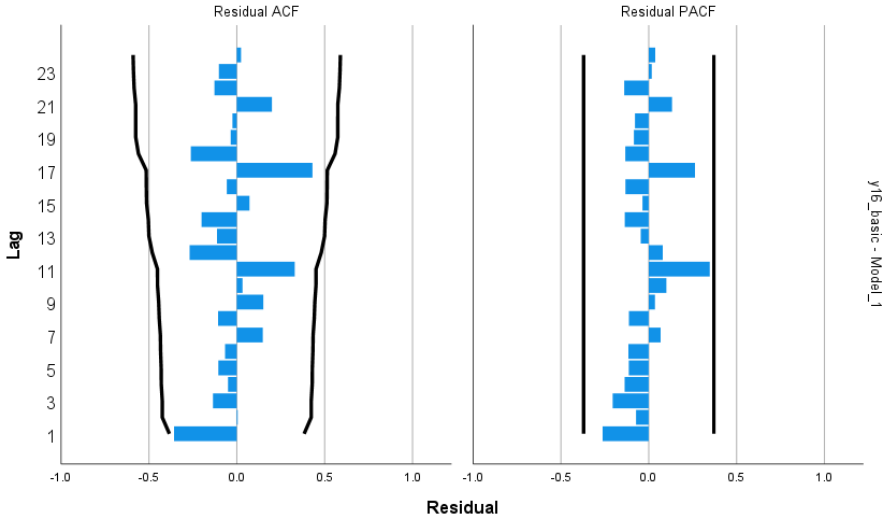
Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.853471	0.106456	17.41073	0.0000
MA(1)	0.669754	0.291932	2.294212	0.0305
SIGMASQ	0.054002	0.019330	2.793608	0.0099

R-squared	0.376671	Mean dependent var	1.876963
Adjusted R-squared	0.326805	S.D. dependent var	0.299738
S.E. of regression	0.245930	Akaike info criterion	0.175645
Sum squared resid	1.512043	Schwarz criterion	0.318381
Log likelihood	0.540972	Hannan-Quinn criter.	0.219281
F-statistic	7.553629	Durbin-Watson stat	1.515257
Prob(F-statistic)	0.002716		

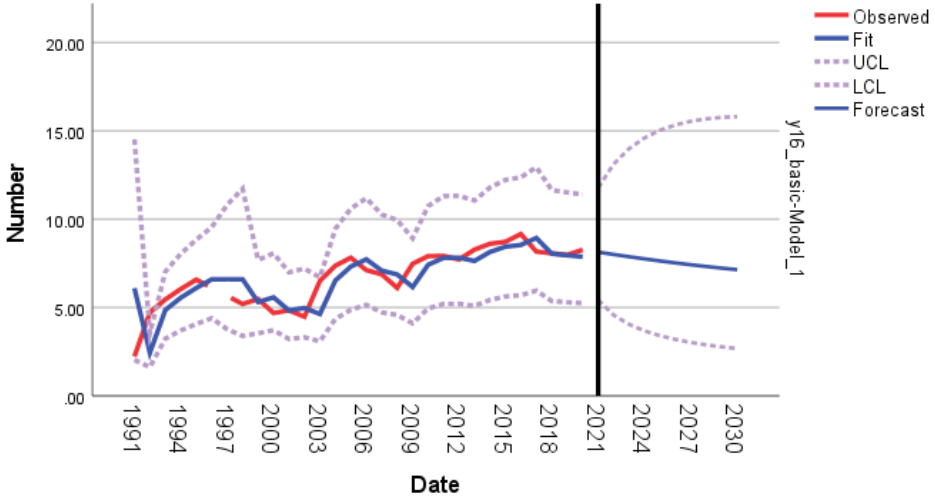
Inverted MA Roots	-.67

The comparison between the three possible models suggests that ARIMA (1,0,0) is the best model as it has the highest R-squared value (0.61).

The residual correlogram shows white noise.



The forecast suggests that the unemployment for people with only basic education will slightly drop for the next decade.

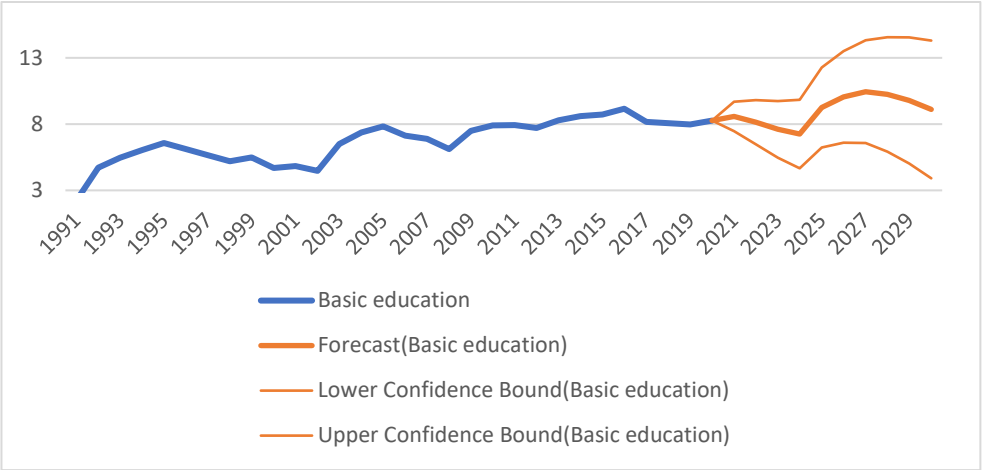


The values of the forecast are presented with the upper and lower bounds.

Year	Forecast	Upper Bound	Lower Bound
2021	4.85	3.69	6.28
2022	4.73	3.32	6.56
2023	4.64	3.11	6.67
2024	4.56	2.98	6.69
2025	4.49	2.89	6.69
2026	4.44	2.83	6.66
2027	4.40	2.79	6.63
2028	4.36	2.76	6.60
2029	4.34	2.73	6.58
2030	4.32	2.71	6.55

The same controversial problem appears here again as the method estimate the unemployment rates to drop. This contradicts with the main findings for the previous unemployment variables. In addition to the issue that people with only basic education are expected to face more difficulty in job market.

The Exponential Smoothing ETS is used for the forecast.



This method captures seasonality which is again not simple to interpret. This method predicts that the rates of unemployment for people with basic education will drop slightly before increasing again to reach a new peak and later will drop again. This is reoccurring visible cycle in the graph.

The forecasted numbers are presented.

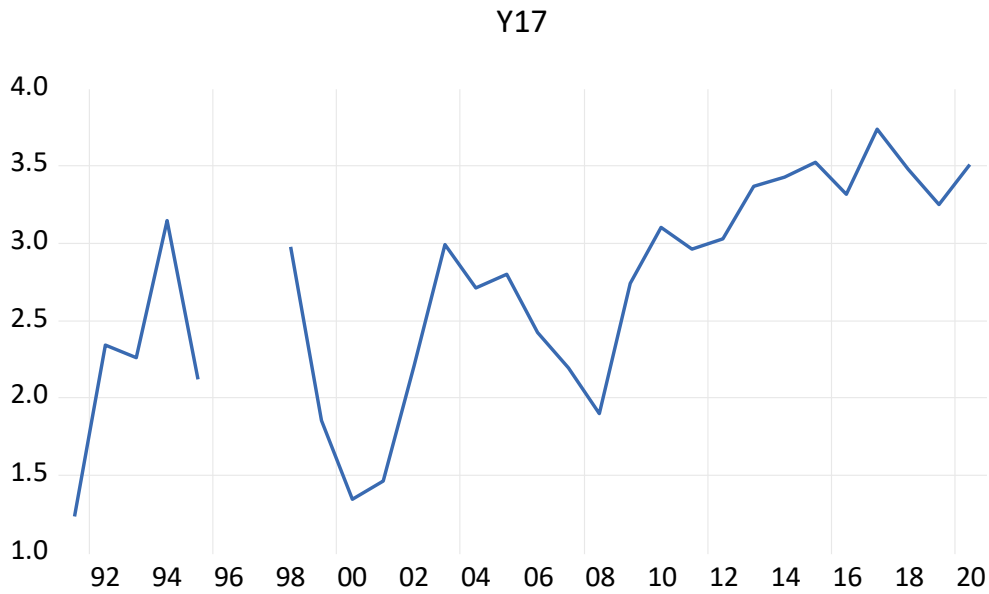
Year	Forecast	Lower Bound	Upper Bound
2021	8.58	7.46	9.69
2022	8.15	6.49	9.80
2023	7.60	5.47	9.73
2024	7.25	4.67	9.83

2025	9.25	6.24	12.26
2026	10.05	6.61	13.49
2027	10.44	6.57	14.32
2028	10.24	5.93	14.56
2029	9.79	5.04	14.54
2030	9.11	3.91	14.31

Exponential Smoothing ETS is more realistic and better repetitive for the historic data and the presumably for the forecasted data.

7.2.17 Modelling unemployment with advanced education y17

Variable $y17$ presents unemployment with advanced education (% of total labor force with advanced education). The plot and the unit root test show that the series is non-stationary



Null Hypothesis: Y17 has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-2.484275	0.1306
Test critical values:	1% level	-3.711457	
	5% level	-2.981038	
	10% level	-2.629906	

*MacKinnon (1996) one-sided p-values.

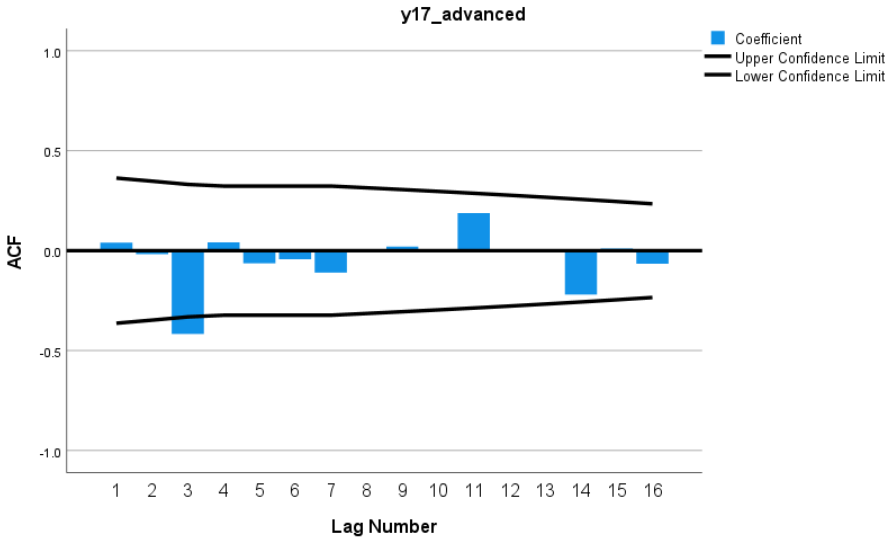
The first order differencing makes the series stationary.

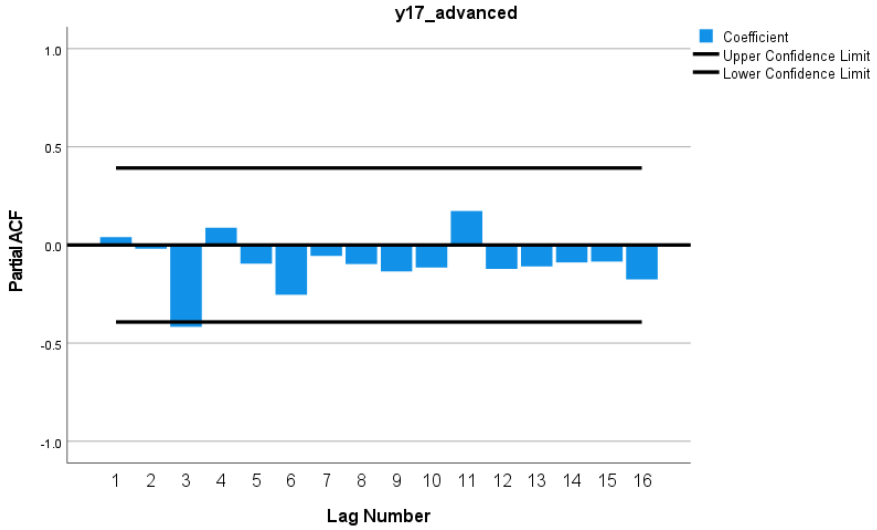
Null Hypothesis: D(Y17) has a unit root
Exogenous: Constant
Lag Length: 0 (Automatic - based on SIC, maxlag=6)

		t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic		-5.518143	0.0002
Test critical values:	1% level	-3.737853	
	5% level	-2.991878	
	10% level	-2.635542	

*MacKinnon (1996) one-sided p-values.

The correlogram of the correlation functions shows that the cut-off appears at the third lag. Therefore, the series will not be further modelled using ARIMA. The trial showed that the second lag and further lags are not suitable for the employment variables.





Just for confirmation, the ARIMA (3,1,0) shows the following model with high p-value for the constant. This model is clearly not suitable, and the series is neither an AR nor a MA process.

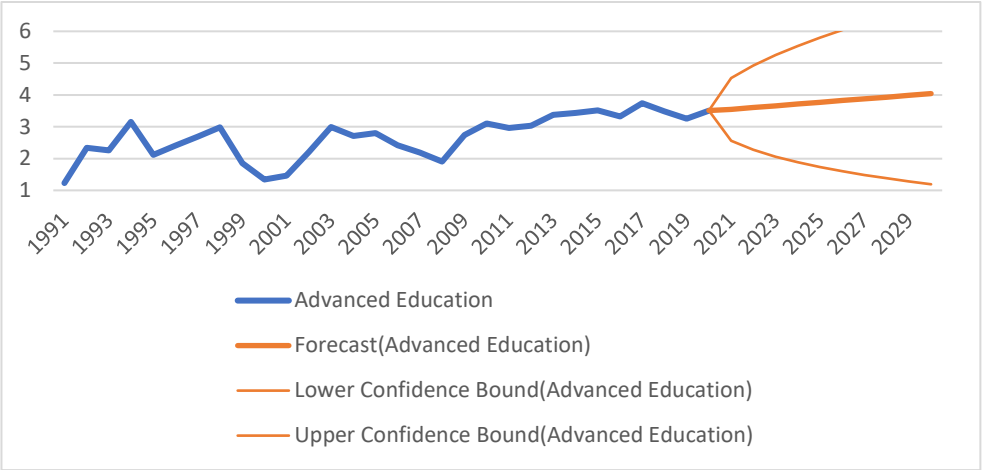
Dependent Variable: D(LY17)
Method: ARMA Maximum Likelihood (OPG - BHHH)
Date: 06/13/22 Time: 13:38
Sample: 1992 2020
Included observations: 26
Convergence achieved after 9 iterations
Coefficient covariance computed using outer product of gradients

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.034984	0.035913	0.974151	0.3401
AR(3)	-0.607734	0.162069	-3.749842	0.0010
SIGMASQ	0.038626	0.011519	3.353250	0.0028

R-squared	0.341145	Mean dependent var	0.027234
Adjusted R-squared	0.283854	S.D. dependent var	0.246924
S.E. of regression	0.208961	Akaike info criterion	-0.095713
Sum squared resid	1.004287	Schwarz criterion	0.049452
Log likelihood	4.244264	Hannan-Quinn criter.	-0.053910
F-statistic	5.954531	Durbin-Watson stat	1.649654
Prob(F-statistic)	0.008243		

Inverted AR Roots	.42+.73i	.42-.73i	-.85

The series will be forecasted using the Exponential Smoothing ETS.



The forecast suggests that level of unemployment for people with advanced education will slightly increase for the coming decade. But it will still be much lower than the rates for people with only basic education.

The forecast values are presented.

Year	Forecast	Lower Bound	Upper Bound
2021	3.55	2.56	4.53
2022	3.60	2.28	4.93
2023	3.66	2.06	5.25
2024	3.71	1.88	5.54
2025	3.77	1.73	5.80

2026	3.82	1.60	6.04
2027	3.88	1.48	6.27
2028	3.93	1.38	6.49
2029	3.99	1.28	6.69
2030	4.04	1.19	6.89

This is the end of forecasting unemployment variables. The research and statistical analysis showed that ARIMA method is not the best method for this type of variables due to their particularity. The Exponential Smoothing ETS is a much stronger and much representative tool for this case. Nevertheless, the forecast could not provide evidence that the future society which is complete IT dependent will come with massive job annulation for the Swiss economy. This is a very promising and reliving finding.

The reminder of the variables will investigate how employment will change in two main sectors, retail sector, and healthcare sector. ARIMA methods will not be considered for these variables for the previously discussed finding.

7.2.18 Forecasting number of workers in retail y18, y19, y20

Notice here that the title has changed from “modelling” to “forecasting”. In the previous variables, the aim was to find the most suitable ARIMA model and identify its parameters. Here, the task is only directly forecasting the variables using Exponential Smoothing ETS.

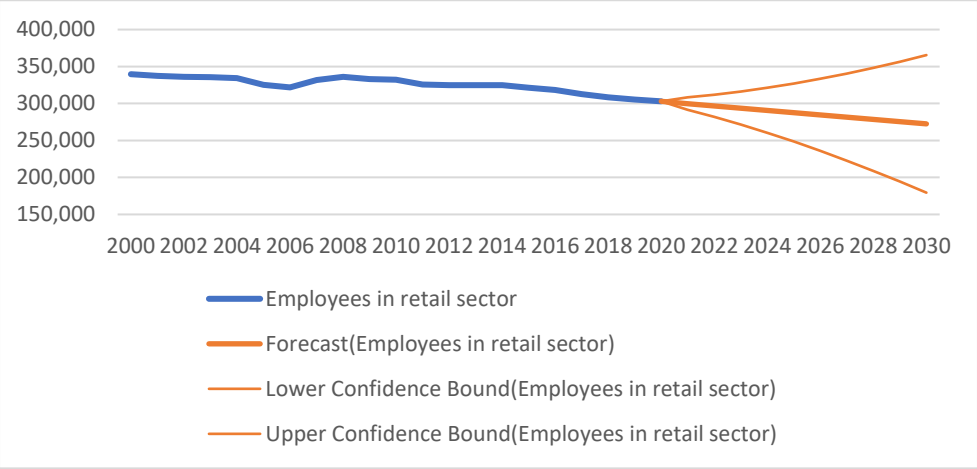
The variables $y18$, $y19$, and $y20$ present the total number of workers in retail sector as total, for male, and for female respectively. The data is published by FSO.

Year	Employees in retail sector	Male employees in retail sector	Female employees in retail sector
2000	339,645	115,194	224,450
2001	337,272	117,036	220,236
2002	336,101	114,913	221,188
2003	335,651	112,744	222,908
2004	334,225	109,428	224,797
2005	325,429	107,850	217,579
2006	321,932	102,870	219,062
2007	331,628	106,131	225,497

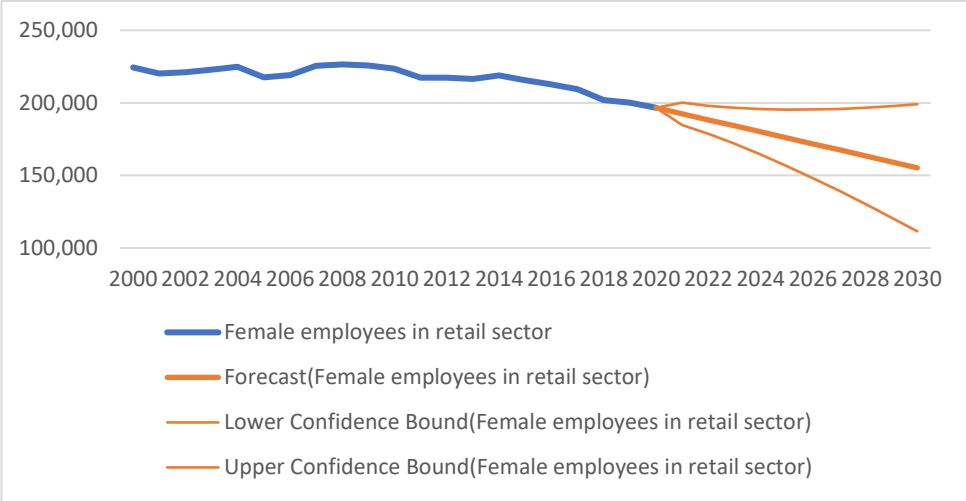
2008	336,228	109,717	226,512
2009	333,160	107,433	225,726
2010	332,010	108,511	223,498
2011	325,696	108,348	217,347
2012	324,740	107,379	217,361
2013	324,741	108,243	216,498
2014	324,836	105,853	218,983
2015	321,355	105,747	215,608
2016	318,158	105,500	212,658
2017	312,750	103,384	209,366
2018	308,359	106,328	202,031
2019	305,528	105,459	200,069
2020	302,945	106,270	196,675

The graph shows a slight drop over the past 20 years in the number of employees in retail sector. There are several reasons behind this drop. The most obvious and IT related is the web shops that are so much in use these days. The consequences of digitalization and the rising trend of online shopping bring changes to the retail sector in positive and negative effects from the perspective of employees. More jobs will be created in the warehouses, IT services, and development for the online shops and the goods delivery, but jobs will be reduced in the physical shops. Nevertheless, no substantial annulation of jobs is expected to happen

unexpectedly in this sector. But still, the forecast confirms that there will be drop in the number of employments in this sector.



The same drop applies for both males and females.



The forecast numbers for all three variables are presented.

Year	Total	Male	Female
2021	299,895	105,694	192,499
2022	296,846	105,243	188,356
2023	293,797	104,792	184,213
2024	290,748	104,341	180,070
2025	287,699	103,890	175,927
2026	284,651	103,439	171,785
2027	281,602	102,989	167,642

2028	278,553	102,538	163,499
2029	275,504	102,087	159,356
2030	272,455	101,636	155,213

Workers in this sector will need to improve their skills and above all IT skills in order to be able to find a job in the future either in this sector which will be more demanding or move to another sector.

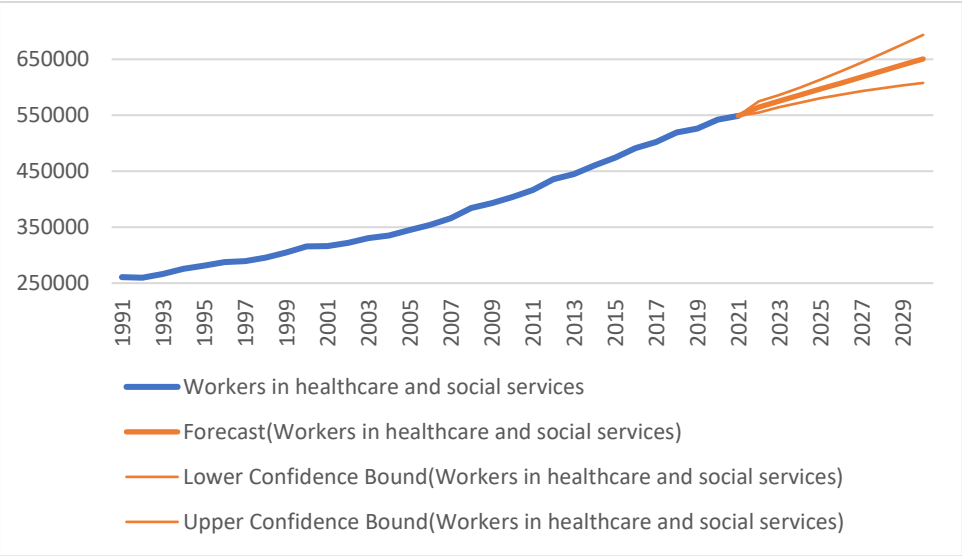
7.2.19 Forecasting the number of workers in healthcare and social work y21

The data is published by FSO and available on quarter bases. The number of the last quarter will be taken for the annual data. Hence, the data is in full-time equivalent.

The data show increased demand in this field of work.

Year	Workers	Year	Workers	Year	Workers
1991	260959	2002	321998	2013	444877
1992	259709	2003	330391	2014	460424
1993	266394	2004	335159	2015	474082
1994	275780	2005	344709	2016	491448
1995	281216	2006	353809	2017	502027
1996	287478	2007	365698	2018	519251
1997	289217	2008	384212	2019	526068
1998	295345	2009	393107	2020	541984
1999	304743	2010	403603	2021	548867
2000	315631	2011	416475		
2001	316028	2012	435530		

The variable will be forecasted using the Exponential Smoothing ETS. The outcomes of the forecast and the values are presented.



The demand on workers in this field will keep growing. Fears of massive job-loss are not realistic, at least in this domain of work. However, these jobs are often not very high paid.

Year	Forecast	Lower Bound	Upper Bound
2022	564566	554618	574513
2023	575330	564212	586447
2024	586093	572716	599471
2025	596857	580204	613510
2026	607621	586862	628380
2027	618385	592848	643921
2028	629149	598276	660021
2029	639912	603223	676602
2030	650676	607740	693613

It is noteworthy to mention that the published data which contain details on the number of workers in most domains shows that sectors like information and communication, and information technology have increasing number of workers every year.

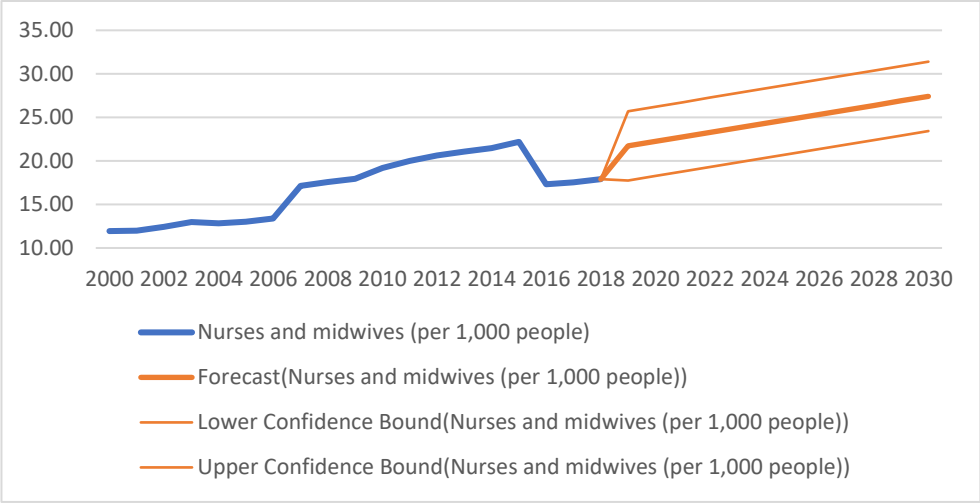
7.2.20 Forecasting the number of nurses and midwives (per 1,000 people) y22

The data is published by the Worldbank from year 2000 until year 2018. It is unfortunate that these data are not available during the breakout of Covid-19.

Year	Figure	Year	Figure
2000	11.94	2010	19.20
2001	11.99	2011	20.00

2002	12.42	2012	20.62
2003	12.97	2013	21.06
2004	12.84	2014	21.48
2005	13.00	2015	22.19
2006	13.38	2016	17.33
2007	17.13	2017	17.54
2008	17.57	2018	17.89
2009	17.96		

As part of the jobs in healthcare, nursing is expected to have increased demand for the coming years. This variable will be forecasted using the Exponential Smoothing ETS. The outcomes and the numbers are presented.



Year	Forecast	Lower Bound	Upper Bound
2019	21.73	17.75	25.71
2020	22.25	18.27	26.23
2021	22.77	18.78	26.75
2022	23.28	19.30	27.26
2023	23.80	19.82	27.78
2024	24.32	20.33	28.30
2025	24.83	20.85	28.81
2026	25.35	21.37	29.33

2027	25.87	21.88	29.85
2028	26.38	22.40	30.37
2029	26.90	22.91	30.88
2030	27.42	23.43	31.40

Despite that the forecast predicts a figure of 27 for year 2030, this does not seem realistic for now. There is missing data for years 2018 through 2022 which affects a new more representative forecast. Besides, it is not easy to predict the impact of technology on the dependency on nurses for the future. However, this sector will continue to provide new jobs for the society and for the economy.

7.2.21 Forecasting economy segments employment shift y21, y22, y23

The next forecast is about variables $y21$, $y22$ and $y23$ which represent the three-sector economy model according to the type of activity.

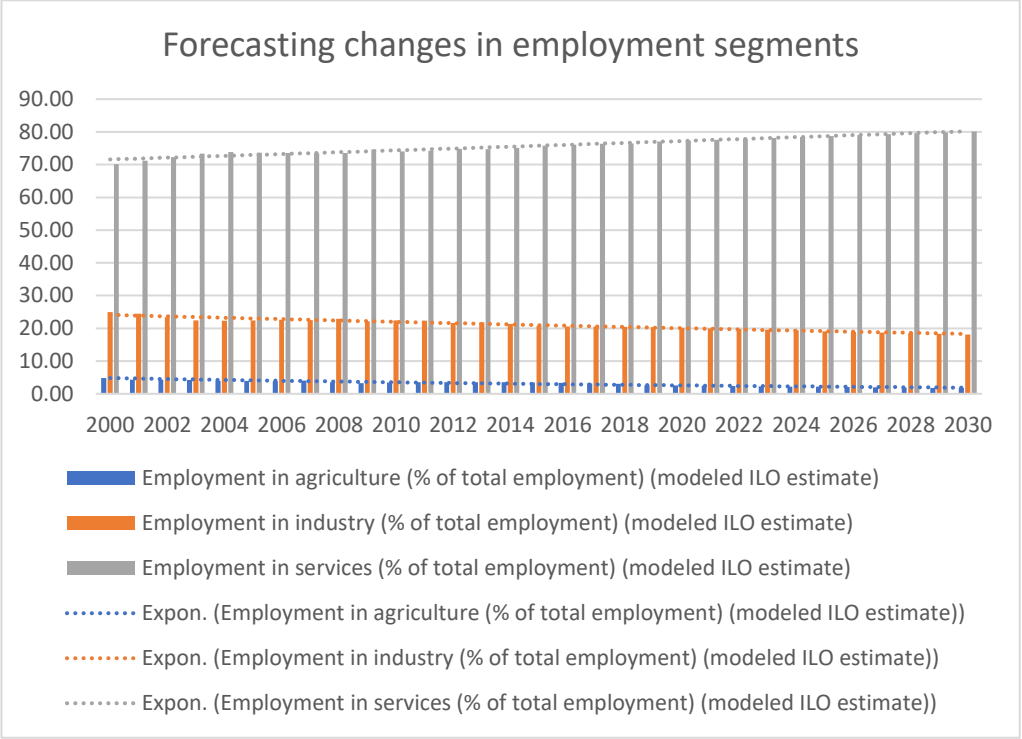
These variables are: $y21$ Employment in agriculture (% of total employment) (modeled ILO estimate). $y22$ Employment in industry (% of total employment) (modeled ILO estimate). $y23$ Employment in services (% of total employment) (modeled ILO estimate).

This model was briefly discussed before. The historic data is published by the Worldbank. The data is presented.

Year	Employment in agriculture	Employment in industry	Employment in services
1991	4.30	29.22	66.49
1992	4.20	28.05	67.75
1993	4.51	27.26	68.23
1994	4.41	27.39	68.20
1995	4.45	28.42	67.13
1996	4.39	26.48	69.13
1997	4.60	25.39	70.00
1998	4.61	25.15	70.24
1999	4.78	24.69	70.53
2000	4.85	25.00	70.15
2001	4.35	24.45	71.20
2002	4.29	23.41	72.31
2003	4.24	22.44	73.33

2004	3.89	22.30	73.81
2005	3.90	22.46	73.64
2006	3.81	22.65	73.54
2007	4.00	22.54	73.45
2008	3.59	22.88	73.53
2009	3.25	22.14	74.61
2010	3.47	22.45	74.08
2011	3.51	22.28	74.21
2012	3.53	21.61	74.86
2013	3.53	21.79	74.68
2014	3.58	21.29	75.13
2015	3.44	20.75	75.81
2016	3.36	20.59	76.05
2017	3.11	20.52	76.38
2018	3.03	20.46	76.51
2019	2.59	20.34	77.07

The outcome of the forecast using Exponential Smoothing ETS is presented in the figure.



The forecast predicts a decline in employment in agriculture and in the industry (as a proportion of total employment), this implies increasing employment in the services sector. For an easier illustration of the forecast outcome, the figure shows the changes in job categories throughout the coming years on a 3 year-base. The result of the forecast is not interpreted

with creating jobs in a sector nor with job loss in other sectors. The forecast is just concerned with job category shifts in society.

The outcome of the forecast matches the historic changes in the three-segment economy model as presented in the previous figure. Considering the unemployment rates forecast and this forecast together, a conclusion comes up which suggests that there will be real job losses in agriculture and industry segments. This will not only be about jobs shifting from a sector to the other. However, the limitation of this forecast revolves around the limitation of the three-segment model was discussed before which makes it harder to interpret where the job losses will be and where the job gains will be. For instance, the forecast tells us that there will be a demand for workers in healthcare in the future but at the same time, there will be a loss in employment in the retail sector. But plugging these inputs in the three-segment model does not return anything because both sectors (retail and healthcare) are considered within the service sector