|  |
| --- |
| IU |
| Computer Science and Society |
| DLBCSCSAS01 |

# Learning Objectives

The Computer Science and Society course teaches the history of computer science as a field of research and application and of the information and communication technology (ICT) developed by computer scientists that increasingly affects everyone’s lives.

The importance of computer science to business and society is presented, particularly in light of how it has been transformed by global networking (the internet, smartphones) and the emergence of new technologies such as artificial intelligence (AI) and military drones. The opportunities offered by these new technologies will be presented, as will the risks.

ICT represents a huge industry and affects almost every aspect of human life. It has contributed a great deal to human progress, but darker sides are also increasingly emerging, for example with regard to data protection or the influence of social media on social discourse. Moreover, technology is evolving rapidly, and the emergence of new technologies such as artificial intelligence raises questions about its impact on society.

Computer scientists who develop ICT and people who use it must be aware of the responsibilities that come with it. Thus, the ultimate learning objective of this course is to enable participants to make ethically sound decisions when dealing with ICT.

# Unit 1 – Computer Science, Society, and the Information Society

**Study Goals**

On completion of this unit, you will be able to …

... explain the importance of computer science to society.

... outline the development of computer science and the Internet.

... name relevant organizations that help shape the field of computer science and society.

# Introduction: Computer Science and Society

## Introduction

Our modern-day society is clearly driven by information. This objection is quite ambivalent, since the information society produces, absorbs, and processes is tremendous and ever-growing amounts of information are encrypted and stored in data sets, but it also depends on the fluctuation and availability of this information. An expanding part of the information society demands access to big data – or at least to some crucial data – to function. Both the principal and side effects of the digital transformation (especially the ever-increasing amount of data production and the utilized data volume in general) accelerate this two-directional data dependency day by day.

The most prominent tool that helps us process the multitude of information sources is of course the computer. Computer science as a scientific discipline has only existed since the late 1940s, but since then it has changed the world in profound ways. After the inception of the personal computer in the 1980s, this tool has become widespread enough to be virtually omnipresent, shaping the world more and more. Computer science encompasses the study of information, computation, and automation. These three components constitute a functional triangle of informatics: Information is data, data is processed by computation, and automation links and triggers these computation processes without intervention. This chapter outlines the evolution of computer science and the technologies it has spawned, and highlights its importance to society from economic and political perspectives.

What is computer science?

Computer science is defined as “the science of systematic processing of information, especially automatic processing with the aid of digital computers” (see Ernst et al., 2020, p. 1). In Germany, it was introduced as a course of study in the late 1960s; in the USA, it has existed as “Computer Science” since the 1940s (ibid., p. 3). Computer science is closely related to mathematics but is also strongly oriented toward engineering. Ernst et al. (2020, p. 2) distinguish four areas of computer science:

1. Theoretical computer science, which deals with fundamentals such as information and coding theory, data structures, and mathematical methods
2. Practical computer science, which is primarily concerned with software development
3. Technical computer science, which studies engineering and physical methods; this area also includes the development of computer hardware
4. Applied computer science, which deals with the use of computers in a practical sense, that is, their use in organizations

The terms “hardware” and “software” long helped to describe the objects of computer science. However, due to the increasing networking of such systems, it is now worthwhile to use other terms. In particular, communication technologies such as networks play a key role, so that today we generally speak of information technology (IT), information systems (IS), or information and communication technology (ICT) (Franzetti, 2019, p. 1). The term “ICT” describes complex systems consisting of hardware and software components and the corresponding network technology.

For example, the Google search engine consists of software (such as the bots that search for information on the internet and the algorithms that organize the search results, but also the data that Google has stored about websites) and hardware (Google operates large data centers to make this data quickly accessible worldwide). In addition, Google builds on the network infrastructure of the World Wide Web (Brin & Page, 1998). The search engine works in concert with these different components.

## Historical Overview of Computer Science and the Internet

Although computer science is a relatively new scientific field, it stems from more than two centuries of fundamental work. First and foremost, mathematicians paved the way for the rise of computing technology. The very first computer scientist may have been German mathematician and philosopher Gottfried Leibniz.

### Gottfried Wilhelm (von) Leibniz (1646–1716)

Leibniz was one of the very rare scientists who rose to fame both as a philosopher and a mathematician. Around 1672 Leibniz invented the first mechanical digital calculator, which he coined the *Stepped Reckoner* (Keates, 2012). The term referred to the calculator’s operating mechanism, called *Staffelwalze*. The stepped reckoner was the very first calculator that could calculate all four arithmetic operations (Beeson, 2004). Leibniz’ invention influenced the development of calculators for at least two centuries.

### Charles Babbage (1791–1871)

The British mathematician, philosopher, and inventor Charles Babbage invented the first mechanical computer back in the 1820s, with an upgraded version following in 1834. Babbage’s invention was coined the *Difference Engine* (with the upgraded variant called the Analytical Engine) (Collier, 1970). The original machine’s name referred to the method of divided differences. This method (originated by Newton) enabled the interpolation of functions through the use of polynomial coefficients. While Babbage’s Difference Engine depended on a human being acting as the algorithm, the Analytical Engine was a general-purpose program-controlled digital computer that worked without human intervention (Hyman, 1982). It was designed to store 1,000 different numbers of 50 digits each – which is more than any computer before the 1960s could store (Collier, 1970). Thus, the Analytical Engine is widely considered as the world’s first programmable computer. It’s worth noting that Charles Babbage was a true pioneer of computer science, since there was no contemporary who envisioned something remotely comparable to Babbage’s vision of a programmable machine.

### Ada Lovelace (1815–1852)

However, the inception of formal informatics, in particular programming, has been credited to Augusta Ada King, Countess of Lovelace and daughter of poet Lord Byron and mathematician Lady Byron. Better known by the name Ada Lovelace, the young mathematician and writer would later be regarded as the world’s first programmer (Collier, 1970). A frequent collaborator of Charles Babbage, Lovelace’s view of his Difference Engine was a more general one, as she considered the machine to be much more than a mere automated calculator: Lovelace also envisioned the processing of music scores, letters, and pictures (Fuegi & Francis, 2003). In other words, Lovelace discovered the computer’s potential as a universal tool.

### Konrad Zuse (1910–1995)

The German engineer and inventor Konrad Zuse has been credited with creating the first universally programmable computer system “Z3” back in 1941 (Rojas, 1997). Zuse was one of the founding fathers of computer science and left behind an impressive and versatile body of work. In one of his books, Zuse even speculated on the possibility of the universe as a giant computer program, a controversial theory that gave rise to the controversial movement of digital physics. Remarkably, Zuse’s Z3 was confirmed to be Turing-complete in 1998, three years after his death (Rojas, 1998).

**Turing completeness**

This refers to the computational universality of a machine. Thus, any Turing machine can be simulated by the given computer. Such a system can run any program, regardless of the programming language. Turing completeness can be viewed as computer science´s most dominant paradigm (Michaelsen, 2009).

### Alan Turing (1912–1954)

The British mathematician and logician Alan Turing has influenced and shaped the rise of computer science itself by formalizing the emerging science of programming. He is the creator of the Turing machine and of the concept of **Turing completeness.** By creating the Turing machine, the inventor paved the way for universal computing. Turing is also considered as one of the early founding fathers of artificial intelligence (AI) and invented the Turing test (the inventor himself preferred “imitation game”) (Turing, 1950). The Turing test is still regarded as a crucial threshold an AI has to overcome to demonstrate a human level of intelligence (Russell & Norvig, 2016). During the Turing test, the testers must decide whether their conversation partner is man or machine. Despite being regarded a national hero – Turing was the leading scientist of the team that decoded the famous ENIGMA code machine of Nazi Germany – he was later sentenced to be chemically castrated due to his homosexuality. In 1954, Turing committed suicide.

### John von Neumann (1903–1957)

Another founding father of modern-day computer science and artificial intelligence was the Hungarian-American mathematician John von Neumann. Von Neumann is most notably credited as the inventor of the von Neumann architecture, a system in which both data and program are binary coded (Goldstine, 1980). He is probably most famous for his conception of an AI-driven technological revolution, which he discussed along with the Polish-American scientist Stanislaw Ulam (1909–1984); von Neumann and Ulam are also the founding fathers of the hypothetical concept of the technological singularity, which is a major theory of transhumanism (ibid.). Theorizing about mankind as the stirrup-holders for a superior technological species itself created, von Neumann’s thought experiment of the technological singularity has further been popularized by science fiction writer and mathematician Vernor Vinge and later by inventor and Google chief engineer Ray Kurzweil.

### Irving John Good (1916–2009)

The British mathematician Irving John Good, a fellow cryptologist who worked with Alan Turing, envisioned a possible intelligence explosion that could lead to an automated but also uncontrollable trajectory of progress. Good’s quote is still controversially debated to the present day: “[…] An ultra-intelligent machine could design even better machines; there would then unquestionably be an intelligence explosion, and the intelligence of man would be left far behind. Thus the first ultra-intelligent machine is the last invention that man need ever make” (Good, p. 1965).

The evolving field of computer science simultaneously describes a historical hierarchy that unfolded during the progress of the developing science. Hence, it was already some sort of quantum leap to move from Babbage’s Difference Engine to his Analytical Engine. The former was a mere highly developed calculation apparatus, while the latter more resembled a modern computer due to its automated functions and independence of human intervention. Arguably, the invention of the Difference Engine back in 1834 marks the very start of computer science, since this was the event where the subject of the science was created.

From there, the art of programming began to evolve to find sound solutions through optimization processes. Most progress was incremental and took years, if not decades, but in the Turing era the development appeared to tangibly accelerate. The phase of rapid progress that began in the 1960s motivated all kinds of hyperbolic claims of technological potential, even leading to the belief that human-like artificial intelligence might be a matter of years away. However, two so-called “AI winters” seemed to deny AI’s announced potential and sowed doubts as to whether the promised powers were feasible at all.

On the other hand, industrial applications revolutionized the business world from the late 1980s, expanding and solidifying the general trust in electronic data processing and increasing its influence as a major driving force of digitization. In particular, ERP systems gained major relevance. Enterprise Resource Planning (abbreviated ERP) is a method that utilizes software to manage major business processes. Typically, ERP is regarded as a type of business management software tool, combined with an organizational unit that collects and interprets data from various business affairs.

### The Advent of the Internet

The internet (a composite constituting of interconnected networks) is a global digital platform that interconnects a vast number of computers and provides access to World Wide Web resources through the use of a web browser. In principle, the internet was installed back in the 1960s as a means of discreet information exchange, mostly for government institutions. After being a) separated from its old context of intelligence affairs and b) substantially expanded, the internet embarked on its unparalleled rise to relevance and influence that we regard as entirely self-evident nowadays.

Originally created on the platform of a packet-switched network, its first iteration was the ARPANET (Advanced Research Projects Agency Network). Back in 1969, ARPANET interconnected the first computers, and one year later the Network Controlling Program got established (Bidgoli, 2004). The usage of these first network systems was almost exclusively military, with a focus on intelligence and espionage applications. Installed as a mutual venture of ARPA (the Advanced Research Projects Agency) and the Defense Communication Agency, while funded by the former and operated by the latter, the internet’s origins were the opposite of civilian (Bigdoli, 2004).

From 1985, the advent of the National Science Foundation Network (NkonuxSFNET) serves as another precursor of the modern-day internet. Commercial websites, networks, and enterprises were integrated into the web structure from the early 1990s, laying the foundations of today’s well-known World Wide Web (www). During the course of this transformative process, a great many innovative and often also disruptive technologies have been implemented. From email correspondence to internet-based telephony (as pioneered by Skype), from websites that enable music (as pioneered by Spotify) and video streaming (YouTube) to blogs, vlogs, and news forums, the internet has accumulated and bundled all information-related enterprises and provides democratic access to the world’s vast pool of information.

In a world of daily growing mountains of data, the means to find the relevant piece of information one is looking for becomes more and more crucial. The advent of the search engine Yahoo in the year 1994 demonstrates in impressive ways the dynamics and unforeseeable reactions of the free market. While Yahoo entered the market as the frontrunner (fueled by the so-called first mover advantage), it quickly showed that being the first isn’t enough. Google, online since 1997 and established as a company in 1998, served the better user experience from day one due to its technologically proficient solutions – for instance, its fully automated usability and its page-rank algorithm. Its design was innovative and unique, and its commercial potential for both private users and companies was invaluable. Nowadays, Google has expanded its business into new fields of research such as artificial intelligence and related fields like self-driving cars. Google is so much more than a search engine now, just as Amazon is so much more than just an online bookstore. Both evolved into multi-layer businesses that also heavily embed and foster AI research. Amazon is the first global player that successfully tailored its business toward recommender systems and predictive analysis. Heavily relying on pattern recognition, Amazon’s algorithms soon rose to fame due to their almost uncanny ability to forecast our next book (or later other item) of interest. With the success of its business model, Amazon soon expanded its core business and continued to do so until today the customer can find virtually any item in Amazon’s catalogue – including even tiny houses.

### Internet of Things; Industrial Internet of Things (IoT; IIoT)

With its unparalleled influence and relevance, the internet has started to leave its digital realm partly behind, since the web has long merged with the physical world. The inception of the Internet of Things (IoT) bridged the gap between bits and bricks, enabling industrial production chains or complex supply chains to be controlled and supervised through internet-based digital technology. The resulting cyber-physical systems are merging digital technology with physical structures, systems, or artefacts.

Cyber-physical systems are of major importance for ICT supply chains; monitoring and control are key functions and play a crucial role in CPS-regulated domains, for instance, in industrial automation systems, telecommunication equipment, smart grids, building controls, digitally driven smart cities, home automation, greener transport, water and wastewater management, health infrastructures, and online public services (Colombo & Karnouskos, 2014).

The Industrial Internet of Things (IIoT) represents the next level of networking; it describes a plexus of interconnected sensors, instruments, and other devices networked together with industrial computer applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially fostering improvements in productivity and efficiency, as well as other economic benefits. The IIoT amounts to an evolution of distributed control systems (DCSs) that allows for a higher degree of automation as well as further increases in efficiency by using cloud computing to refine and optimize the process controls.

An IIoT business case from Germany is the Munich-based start-up Konux. Specializing in AI-monitored rail points control systems, Konux tailors its solutions for railroad demands. The successful start-up is entertaining cooperations with Deutsche Bahn, but also with Sweden and China. Enabling a cost-efficient 24/7 monitoring of the rail switches – compared to merely occasional checks – will result in increased safety and efficiency, ultimately resulting in an increase of profitability.

The Fourth Industrial Revolution (4IR/Industry 4.0) describes a rapidly changing economic environment predominantly shaped by progressive networking, expanding automation processes, and growing interconnectivity. Popularized by World Economic Forum founder Klaus Schwab, Industry 4.0 clearly marks more than a linear progression in efficiency for him; instead, Schwab considers the Fourth Industrial Revolution as a shift of paradigm in industrial capitalism (Philbeck & Davis, 2018).

The internet is not only the platform enabling Industry 4.0; there is also the trio of new realities, namely virtual reality (VR), augmented reality (AR), and mixed reality, which all adds up to extended reality (XR). Virtual reality is a computer-generated environment that utilizes visuals (3D) and in some applications also sound. Although there are VR applications that work with huge screens and special rooms (CAVE, abbr. for Cave Automatic Virtual Environment), the more widespread and much more cost-efficient variant is brought to the consumer by 3D goggles (Kottila, 2014). Highly immersive, VR started off in the gaming industry but didn’t stay limited to this sector. In contrast to virtual reality, augmented reality doesn’t supplant actual reality entirely but overlays certain functions, like additional information and virtual objects. Germany-based AR developer Wikitude offers an application that identifies the current location with GPS and adds background information on the area. Mixed reality merges physical reality with the digital world, adding virtual elements to natural perception. All three technologies aren’t bound to the gaming sector, since there are many industrial applications, even in the brick-and-mortar domain.

**Metaverse**

The metaverse is the sum of all virtual environments and 3D animated realities that are accessible by the internet. Coined by American SciFi author Neal Stephenson in his 1992 novel “Snow Crash,” the metaverse became a buzzword in October 2021, when Facebook CEO Mark Zuckerberg rebranded the company into Meta and invested billions of dollars in the metaverse.

The internet is also the portal to the **metaverse** – a nested hierarchy of simulations in digital environments that has notable commercial potential and will very likely establish another novel form of industry. Right now, the metaverse is merely in its pioneering days, but with international market leaders like Adidas and Nike investing billions in virtual sneakers and digital flagship stores, the gold rush mood is already tangible.

With the installation and the widespread social acceptance (and even dependence on it), the World Wide Web is now undeniably the most dominant software platform in the world. Sadly, the importance of a technology can easily be abused, and thus the internet is censored or partly turned off in restrictive countries like Iran. The free flow of information and the inherent democratic powers of the World Wide Web are undermined by dictatorships. While clearly a modern-day innovation, its visionary roots trace back to the time when von Neumann and his fellow scientists dominated the flourishing field of computer science.

But the mere idea of an all-connecting network is, remarkably, older. Of all things it was a Jesuit priest named Pierre Teilhard de Chardin who not only anticipated the inception of the internet decades before its advent but also even elaborated on transhumanism long before the term was even founded. What de Chardin called the noosphere describes a highly interconnected world where minds are directly networking and ideas are freely flowing (deChardin, 1925). While some aspects of the noosphere apply rather to globalization, others indeed seem to describe the internet – decades prior to its advent.

The Metaverse is the sum of all virtual environments and 3D animated realities that are accessible by the internet. Coined by US-american SciFi author Neal Stephenson in his 1992 novel „Snow Crash”, the metaverse became a buzzword in October 2021, when Facebook CEO Mark Zuckerberg rebranded the company into Meta and invested billions of dollars in the metaverse.

### Self-check questions

1. Name three major founding fathers of computer science (Babbage, Turing, von Neumann)
2. How did google win over yahoo? (user experience, design, algorithm, vision)

## Computer Science, Society, and the Information Society

In view of the growing importance of information and communication technologies (ICT), the term “information society” has been discussed, especially since the 1980s. The background to this was the assumption that the distribution of economic sectors would change in such a way that the information economy should be seen as a separate sector (alongside the established sectors of agriculture, industry, and services) (Schmiede, 2013, p. 1). It had been noted that “the sectors of the economy that either directly produce information and information technology or do so indirectly, in the form of organization, service, management, or bureaucracy, are primarily concerned with the collection and dissemination of information – already accounted for about half of the US workforce in 1980[n]” (ibid.). The information society is molded, shaped, and designed by digital technology and in particular its unparalleled abilities to provide access to and to process huge amounts of data. Industry 4.0 and the Industrial Internet of Things (IIoT) bridges the gap between the physical world and the digital realm, enabling an entirely new level of efficiency and productivity. On the other hand, social media has not only become a billion-dollar market in its own right but has evolved into a major influence in terms of society and even politics. Social norms and standards have been constantly questioned through social media in an attempt to alter these normative constellations.

There are a great many misconceptions surrounding the growing field of computer science. The reason people develop borderline superstitious ideas is simply a result of a widespread tendency to anthropomorphize technology. For instance, people tend to drastically over- or underestimate the properties and potentials of the computer as a universal tool in general. While skepticism often focusses upon the capabilities of current devices, people tend to overestimate the powers of next-generation computers. Irrational fears of technological takeover scenarios co-exist with widespread notions of computers as pseudo-sentient entities that seemingly work – or fail to work – as they please. Such notions are easy to debunk, since they stem from a lack of digital literacy. The ability to understand and use information in multiple formats from a wide range of sources when it is presented via computers summarizes digital literacy (Gilster, 1997). Although there is no general definition that counts for everybody, digital literacy requires “foundational skills that provide access to infrastructure which are built on to have personal meaning and relevance” (Beetham, 2009, p. 28). At the same time, there is an utter lack of understanding as regards the real working principles of computer technology. The more advanced and less widespread the technology is, the more opaque its core functions tend to become for the general public; hence, the abyss of misunderstandings and misconceptions can grow even deeper.

This tendency is clearly evident in the context of more advanced technologies like recommender systems and their specific capabilities; for instance, recommender systems really don’t anticipate the future when they predict decisions. Instead, recommender systems rather work on the sole basis of pattern recognition. Hence, the predictions of these systems are based on empirical data that has been gained in advance. Without initial information about an individual’s items of interest, such a system cannot really recommend anything specifically, and even with access to previous decisions it is merely an estimation based on the empirical data and the identified patterns (Lierfeld, 2022). However, humans tend to anthropomorphize technological capabilities and would rather believe the system knows their real wishes better than themselves than accept the mundane truth that recommender systems merely interpret data and guess outcomes – albeit often with a high level of accuracy. However, recommender systems can also utterly fail, because people’s subjectivity still constitutes a tremendous uncertainty that cannot be solved by mere calculus.

These skewed perspectives result in vast ignorance of the actual aspects and factors of how computers work. This growing ignorance leads to crude views, an inappropriately metaphorical language, and even superstitious conceptions that stand in stark contrast to objective reality. Thus, on the educational side, one of the major driving forces of computer science should be the aim to increase digital literacy and establish a fact-based understanding that avoids the false and deceitful metaphors that are so widespread in the general population.

Utter misinformation surrounds not only computer science but the whole field of informatics like weeds, with a special emphasis on artificial intelligence. Often labelled as incompatible with human intelligence or even portrayed as a fundamental hazard to the mere existence of humanity, AI is probably the most misunderstood branch of informatics (Russell, 2016). There is indeed a tremendous gap between the characteristics of biological intelligence and machine-based cognition. This skew is mostly established through one of the major strengths of artificial intelligence, namely its pattern recognition skills. But although the gap is undeniable, it may be bridged. As Lierfeld proposed in 2019, biological and non-biological forms of intelligence work on diametrically opposed skills:

Human intelligence excels by deriving a maximum of relevant conclusions from a minimum of information.

Machine intelligence excels by deriving a minimum of relevant conclusions from a maximum of information (see Lierfeld, 2019).

Both definitions aren’t merely playing around with formalities to create a chiasmus that suggests incompatibility. In fact, these definitions suggest a high degree of complementariness between both cognitive systems: while human beings are able to create inventions just by combining two relevant pieces of information (e.g., the combination of information 1 “friction leads to heat production” and information 2 “certain material is able to store and transfer heat better than others” inevitably led to the invention of fire starting (ibid.)).

On the other hand, machine intelligence is able to find the needle in the information haystack due to its highly developed, accurate pattern recognition skills. These strengths stand in stark contrast to the skill sets of most humans; only some autists or savants can pull off comparable cognitive feats. In general, we humans aren’t blessed with the skills that are in need to handle huge amounts of data: we are far better suited to improvising a way to burn the big haystack than to finding a tiny needle in it. Acknowledging the respective strengths and deficits of both biologically based and machine-based cognition will not only enable a much more effective cooperation but will also lead to stronger results, ultimately showing how AI and human intelligence are complementary rather than incompatible.

Encouraging research, enabling the general population to understand the facts behind digital information processing, and spreading digital enlightenment are thus mandatory to fighting such forms of modern-day technology-based superstition and fostering digital enlightenment.

Even if the information economy has not established itself as a new sector in the economic analysis, it is clear that a shift toward services has taken place within the economic sectors and is continuing. A large part of this is likely to be accounted for by the information economy in this sense.

Employees by Economic Sector

Chart, bar chart

Description automatically generated

Source: Bundeszentrale für politische Bildung, <https://www.bpb.de/nachschlagen/zahlen-und-fakten/soziale-situation-in-deutschland/61698/erwerbstaetige-nach-wirtschaftssektoren>

### Self-check questions

Please answer the following questions:

1. What are the major branches of computer science? (information, computation and automation)
2. What is the main difference between biological and non-biological intelligence? (AI skilled in pattern recognition, human beings use intuition)

## Relevant Organizations

The following chart provides an overview of computer science’s leading international organizations.

|  |  |
| --- | --- |
| International Organizations | |
| **Name** | **Mission Statement** |
| American Society for Information Science and Technology (ASIS&T): | Among its some 4,000 members, ASIS&T counts information specialists in computer science, management, engineering, law, medicine, chemistry, and education. The society is committed to finding new and better theories, techniques, and technologies to improve access to information. |
| Association for Computing Machinery (ACM): | Founded in 1947 as an international scientific and educational organization dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests. |
| [Computing Research Association](http://cra.org/): | Its focus is “to enhance innovation by joining with industry, government and academia to strengthen research and advanced education in computing.” |
| IEEE (Institution of Electrical and Electronics Engineers): | “World’s largest professional association for the advancement of technology” |
| Association for Women in Computing: | “One of the first professional organizations for women in computing” focused on “promoting the advancement of women on the computing professions” |
| American Society for Engineering Education (ASEE): | “ASEE advances innovation, excellence, and access at all levels of education for the engineering profession.” |
| IET (Institution of Engineering and Technology): | “To inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society.” |

The following chart provides an overview of Germany’s leading computer science organizations.

|  |  |
| --- | --- |
| Germany-based organizations | |
| **Name** | **Mission Statements/Description** |
| Gesellschaft für Informatik: | Support of ICT workforce; mold the further development of informatics.  Many IT professionals are aware of the responsibility for the consequences of their actions. Thus, their most important professional association in Germany, the Gesellschaft für Informatik e.V. (GI), which was founded in 1969, repeatedly takes a stand on social issues. |
| KI Bundesverband e.V. | Started in 2020, the KI Bundesverband strives to foster ethical solutions and implement a mutually beneficial AI development. |
| Fraunhofer Institute for Intelligent Analysis and Information (Fraunhofer IAIS) | This deals with ethical and societal issues. Cooperation between Fraunhofer IAIS and the Federal Office for Information Security BSI. Developing a technological evaluation method for the certification of AI systems. |
| Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF) | In addition to the GI, there is the Forum Informatiker:innen für Frieden und gesellschaftliche Verantwortung (FifF), which deals with ethical and social issues and also cooperates with the GI at events. |

### Self-study questions

Name and describe one national and two international organizations of computer science:

*National:*

*Gesellschaft für Informatik: Support of ICT workforce; mold the further development of informatics*

*KI Bundesverband e.V.: Started in 2020, the KI Bundesverband strives to foster ethical solutions and implement a mutually beneficial AI development.*

*KI NRW: An initiative to foster progress and the political regulation of AI.*

*FifF: the Forum für Frieden und gesellschaftliche Verantwortung deals with ethical and societal issues.*

*International:*

*American Society for Information Science and Technology (ASIS&T): Among its some 4,000 members, ASIS&T counts information specialists in computer science, management, engineering, law, medicine, chemistry, and education. The society is committed to finding new and better theories, techniques, and technologies to improve access to information.*

*Association for Computing Machinery (ACM): Founded in 1947 as an international scientific and educational organization dedicated to advancing the art, science, engineering, and application of information technology, serving both professional and public interests.*

*Association for Women in Computing:„One of the first professional organizations for women in computing”focused on „promoting the advancement of women on the computing professions”*

[*Computing Research Association*](http://cra.org/)*: Its focus is “to enhance innovation by joining with industry, government and academia to strengthen research and advanced education in computing”*

*IEEE (Institution of Electrical and Electronics Engineers): “world’s largest professional association for the advancement of technology”*

*American Society for Engineering Education (ASEE): „ASEE advances innovation, excellence, and access at all levels of education for the engineering profession.”*

*IET (Institution of Engineering and Technology): “To inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society.”*

## Summary

In recent decades, computing and the information and communication technologies (ICT) it has developed have significantly changed society and the lives of individuals. In particular, with global networking through technologies such as the World Wide Web and smartphones, individuals now have access to data and services that were unthinkable just a short time ago. The term “information society” reflects how important data and information are in our society. ICT is a key driver of prosperity and progress. At the same time, these technologies are increasingly interfering with various aspects of life and can thus affect individual freedoms, jobs, or the well-being of the planet. Civil society organizations serve as a link between the individual or individuals and society. They critically accompany the development of information technology.

# Unit 2 – The Role of Data in the Information Society

**Study Goals**

On completion of this unit, you will be able to …

… name hazards of the information society.

… understand crucial aspects of data generation and data protection.

… describe the functioning of industry-shaping systems like ERP systems or cyber-physical systems (IoT).

… discuss data as a commodity.

# 2. The Role of Data in the Information Society

## Introduction

The amount of data produced worldwide has been growing rapidly for years. How is data created and what are its commercial benefits? What is the importance of protecting the privacy of individuals and how is this regulated? What interest do states and companies have in collecting data from individuals? And how can we ensure that our data can still be used by future generations?

## 2.1 Data as a Commodity

### What is Data?

Data is defined here as signs in a rule-based context. When it is enriched with a context and thus acquires meaning, it is referred to as information, which in turn is the basis for knowledge (Krcmar, 2015, p. 11). With the advancing digitization and networking of all areas of business and private life, data is increasingly accumulating frequently and in large quantities. At the same time, there are now powerful tools for analyzing even large volumes of data in real time. Thus, the collection and analysis of data is of outstanding importance for organizations. As the basis for many sectors of the economy, data has even been compared to oil: “Data in the 21st Century is like oil in the 18th Century: an immensely, untapped valuable asset. Like oil, for those who see Data’s fundamental value and learn to extract and use it there will be huge rewards” (Toonders, 2014).

The metaphor of the “new oil” illustrates well the economic value of data, but it also has its limitations. For example, critics point out that unlike oil, data is potentially infinitely available and is not a commodity but is processed individually for the respective application purpose (Maicher, 2016). Additionally, it can be copied at almost no marginal cost. Thus, data is “much more valuable than oil or gold, namely infinitely valuable” (Bendig, 2020). This makes it clear that the collection and analysis of ever-increasing amounts of data, as well as the protection of individual privacy, raise issues of great importance for society. Aspiring computer scientists must therefore also address ethical issues in dealing with data.

Data is undeniably the major industrial driving force of the present day as well as the foreseeable future. With its push to make data sharable and accessible, digitization is the societal engine that drives our collective data dependency further. In the meantime, every individual in the information society has an internet footprint that consists of

* search history,
* online purchasing,
* online discussions,
* hotel or flight booking,
* social media habits, and
* much more data.

This collection of data can make our next steps anticipatable, but at minimum our scope of interest and our budget have been identified. With this knowledge, advertising can be much more tailored to the assumed or factual needs of the individual customer. As a result, sales expand and advertising evolves to formerly unparalleled levels of precision.

### Data Mining

Marketing scholars increasingly use web scraping and application programming interfaces (APIs) to collect data from the internet (Boegershausen et al., 2022). Data mining is the process of identifying patterns in vast data sets, often “big data.” Through the means of data mining, users are analyzed based on their previous online behavior. The extracted patterns can be further processed and utilized, for instance, to tailor advertising to the interests of the individual user. It’s this quality to precisely address a target group or even individual that makes algorithm-based online marketing so powerful. Data also helps to evaluate the success of a campaign, a particular method or strategy. Of course, the generated data has to be interpreted, but the output can be used to plan future scenarios.

Data has evolved to one of the world’s most important commodities over recent decades. This is mainly due to the rising profits achievable through the means of data usage. Personalized item offers, as enabled by recommender systems, make true niche marketing possible. Algorithmic decision making automates a great many administrative functions, rendering people increasingly obsolete in the decision chain. High-frequency trading algorithms create the trader’s profits due to the algorithm’s ability to trade in timespans of microseconds. In general, the potential for revenue is exceptionally high with the use of big data (Lee & Chen, 2021).

Because personal data is especially valuable, it warrants particular protection. But despite the efforts of the DSGVO in Europe and the 2018 Data Protection Act in the USA, it’s still possible to sell and purchase certain data. Companies like Tesla are more data enterprises than car producers, with 25 gigabytes worth of data per hour emitted by every driving Tesla model. After the platform-based internet era that was established with Web 2.0, we have now entered the next stage with Web 3.0 and its linkages to the metaverse.

Cryptocurrencies and non-fungible tokens (NFTs) expand and strengthen the view of data as a commodity. There is no gold standard in the world of cryptocurrencies; the free trading market represents all its worth. However, the value added is substantial, and while the lead cryptocurrency Bitcoin dropped more than 50 percent recently, its major rival Ethereum prospers, and cryptocurrencies boom in general. Meanwhile, the prices for land in the metaverse are skyrocketing. For example, a piece of virtual land next to US rapper Snoop Dogg’s mansion is worth $450,000 (Sackmann, 2022). This is particularly interesting because the metaverse is a digital 3D counter-world created wholly from data. But this data is revealed to be very valuable. However, after initial multi-billion investments, most notably by Adidas and Nike, metaverse investments have decreased by the end of 2022 due to the recession. In general, it will take more time to develop a common understanding of this new digital realm.

### Data Economy in Numbers

To give a more visceral impression of how impactful the commodities data and in particular big data really are, let’s look at the annual revenues that Germany generated through big data. It has been estimated that the German economy aggravated around 6.4 billion euros in the year 2018 through big data alone (Statista, 2018). Big data-related hardware sales figure 600 million euros, while software sales accumulate to roughly 2.9 billion euros. The correlating data volume is disproportionately growing in comparison to the rising revenues; ironically, the exploding big data business seems to even lack behind the ever-expanding stacks of data we produce, process, and handle every day. While the worldwide generated and/or replicated volume of data was figuring 6.5 zettabytes back in 2012, in 2018 it was 33 zettabytes and in 2020 it’s already 64.2 zettabytes. For the year 2025, the annual generated data volume will be an estimated 181 **zettabytes** (International Data Corporation, 2021).

**Zettabyte**

One zettabyte equals 1 trillion bytes or 1 billion terabytes. In numbers, 1 zettabyte looks like this:

1,000,000,000,000,000,000,000 bytes.

### Social Media

A great deal of data is generated by the various social media apps, which offer various posting formats such as news feeds, reels, stories, or shorts. Turning into a business model for lifestyle companies, who install popular influencers to multiply their sales, social media platforms encourage users to frequently upload content in order to stay or become noticed. Ironically, the rapidly evolving social media ecosystem is potentially harmful for the biological ecosystem, regarding how energy-consuming the daily activities of the more than 4.26 billion people (2021) engaging in social media are (Dessai & Palandrani, 2022). The carbon footprint of social media is deep and dirty, and this highlights a complex ethical dilemma. Should we regulate the production of content, for instance, by utilizing algorithms that prefer substantial, possibly scientific content over pranks or other trivial forms of “click bait entertainment”? Or should we even restrict the volume of content production to a certain threshold? Given the momentum of current developments and the tangible hazards of the climate crisis, there is clearly a need for future regulation of some sort.

Data as a commodity will accompany every aspect of life, and its universality will lead to ever-new business models that find novel ways to monetarize all kind of data.

1 zettabyte equals 1 trillion bytes. In numbers, 1 zettabyte looks like this:

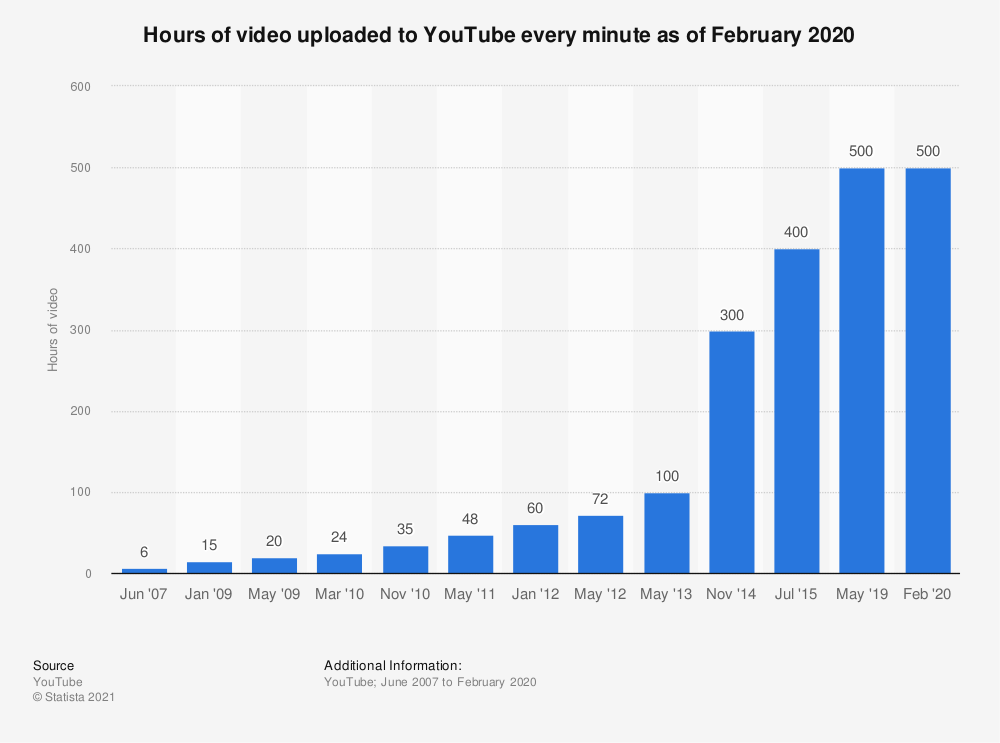
1.000.000.000.000.000.000.000

1 zettabyte equals 1 billion

### Data Generated Worldwide

Also, the number of videos uploaded to the online platform YouTube is very interesting in this context – this is traditionally measured in hours of video content uploaded per minute. This value last stood at 500 (2020, before the COVID 19 pandemic).

YouTube Uploads per Minute

 Source: Statista, <https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/>

There are several reasons for the growth in the amount of data worldwide.

The most important data sources are (AAPOR, 2015)

* social media data (e.g., chats, tweets).
* personal data (e.g., records of sports activities, browsing and search history).
* sensor data (e.g., from smartphones, cars, or manufacturing plants).
* transactional data (e.g., data about business activities in ERP systems).
* data collected by the administration or other government agencies (e.g., registration data or data from tax returns).

It is noticeable that, as a result of digitization, information that was previously only available in analog form is now increasingly available digitally. In companies in particular, ERP systems cover finance and accounting, human resources, materials management, logistics, production, and sales (Miebach, 2020, p. 123), collect the data and make it accessible for further analysis.

In addition, sensors that continuously generate data are being used in more and more places. These are important in industrial production – for example, RFID tags (Radio Frequency Identification) allow the position of individual objects (such as automotive parts or packages) to be tracked (Krcmar, 2015, p. 707f.). Sensors are an important basis for smart factories, which are discussed under the buzzword Industry 4.0 (Miebach, 2020, p. 146f.).

Private individuals are also increasingly surrounded by sensors. A typical smartphone, for example, has a camera, a microphone, a GPS sensor for geographic location/navigation, a motion sensor, etc. Together with smartphone usage data (conversations, chat logs, app usage), this creates a complete picture of the user’s actions. This should initially be seen in a value-free way – there is, for example, the “Quantified Self” movement, whose followers specifically collect as much data as possible about their lives (e.g., using fitness trackers and smartwatches) to optimize aspects such as weight, blood pressure, etc. (Mämecke, 2021).

### Data in Organizations

For as long as information systems have existed in organizations, data has been collected and analyzed. As technical capabilities increase, so do the opportunities to collect and analyze data (see Alpar et al., 2019). A significant part of the information systems story deals with the growing amount of data in organizations and technical ways to analyze it. Decision support applications draw on existing data within the organization to generate new insights. In this way, they can support decision-makers at the management level of the organization (e.g., with dashboards, i.e., user interfaces that display the most important key figures of the company in real time) or make decisions automatically (e.g., about granting a loan) (Alpar et al., 2019, pp. 269–278). Data warehouse systems established themselves as early as the 1980s, creating a central “warehouse” for corporate data to support decision-making processes (Alpar et al., 2019, p. 278). What is new is that artificial intelligence technologies can be used to automatically generate knowledge from large amounts of data (“data mining”). The growth in the amount of data and the increasing need for real-time analysis has led to a number of technologies that enable such analysis (e.g., new types of powerful databases). These are summarized under the term “big data.” The industry association Bitkom defines the term thus:

Big Data supports the economically meaningful extraction and use of decision-relevant insights from qualitatively diverse and differently structured information that is subject to rapid change and is available to an unprecedented extent. (Bitkom e.V., 2012, p. 21)

Big data technologies were co-developed to a large extent by large internet corporations that have access to enormous databases and depend on rapid analysis of this data, e.g., Amazon (e-commerce), Google (search engine), and Facebook (social network) (Miebach, 2020, p. 244).

The ethical background to the use of data continues to gain importance with the advent of artificial intelligence, as this technology enables systems that can increasingly mimic human capabilities such as rational thought and action based on data and thus make far-reaching decisions (Miebach, 2020, pp. 185–193).

### Business Based on Personal Data

With the advent of the World Wide Web and, in particular, big data technologies, private companies began to collect more and more extensive data about individuals. The search engine company Google originally aimed to collect and analyze the information on the World Wide Web (Brin & Page, 1998). This is still reflected in the company’s self-presentation: “Our mission is to organize the world’s information and make it universally accessible and useful” (Google.com, n.d.). In addition, Google developed increasingly personalized services such as Gmail (e-mail service) and Google Maps (maps and navigation) and began to collect data from users to offer them better services (and more relevant ads). Today, internet companies have data sets about their users that would have been unimaginable decades ago. These data sets form a central part of their business model.

Companies may have a legitimate interest in collecting data about their users, and to a certain extent it is in the common interest. For example, a large fraction of the services and content on the internet is still free and financed by advertising. Google’s search engine was a pioneer in this respect: It was only through the introduction of AdWords, i.e., ads that match the respective search term, that the young company was able to secure a source of income (Battelle, 2005). Google is transparent about what data it collects and for what purpose, arguing that this activity is beneficial for users as it allows them to be offered personalized services and more relevant search results, among other things (Google, 2021).

Internet companies such as Google and Facebook also promise not to sell their users’ data. Nevertheless, the trade in personal data (from other sources) is a lucrative business. The volume of the market for address and data trading in Germany was around 610 million euros in 2014 (Goldhammer & Wiegand, 2017). Companies buy this data for many reasons, e.g., to better understand the purchasing behavior of their customers and to increase sales through improved recommendations (Čas & Peissl, 2010).

The international market for data trading is correspondingly larger. Latto (2020) puts it at $156 billion a year. The case of the company Cambridge Analytica, which obtained data from Facebook users in a dubious manner and used it for political microtargeting, i.e., targeting people who are receptive to certain political messages (Dachwitz et al., 2018), caused a sensation. The events are also echoed in the documentary “The Great Hack” (Amer et al., 2019).

Estimates of the value of an individual’s data range from $40 to $240 per year (Latto, 2020). An overview of the many methods of data collection and aggregation is shown in the figure below:

Data collection on customers

Chart, bubble chart

Description automatically generated (Source: Cracked Labs (CC BY-SA 4.0), <https://crackedlabs.org/en/corporate-surveillance/infographics>

### Collecting User Data

Conscious handling of personal data is therefore necessary. In principle, users of free online services should keep in mind the principle: “If you are not paying for it, you’re not the customer; you’re the product being sold” (Quote Investigator, 2017). Shoshana Zuboff even argues, “You are by no means the product, but merely the free source of the raw material that is processed into marketable products” (Zuboff, 2019). She speaks of “surveillance capitalism,” in which the “experiences of private people are declared the free raw material for production and sale,” and points out the dangers this poses to society and the well-being of individuals.

### Self-check questions

1. Please complete the following statements:

In 2020, 500 hours of video content were published on YouTube every minute.

1. Please complete the following statements:

Technologies for evaluating large amounts of data in real time are also referred to as Big Data.

1. What are the goals of data mining? (Identifying and extracting crucial patterns)
2. Give 2 examples of data as a commodity (data mining, recommender systems)

## 2.2 Data Protection and Data Spying

With data representing crucial information about individuals, companies, or political institutions, it is mandatory to render the data inaccessible to third parties. In reality, it is highly idealistic to believe data security can be managed to grant complete protection. Countless publicly covered leaks have made the security issue obvious, exposing how vulnerable even government institutions are to data theft and hacking. A great many leaked emails have ended careers, nourished the yellow press, and made everything contained public domain – from personal preferences to relationship status to financial conditions. Hence, the protection of data has evolved into a field in its own right. Data protection must not be mistaken for data security though. While the former is a legal act, the latter describes its technological implementation.

Cybersecurity is the official term for any professional activity that aims to protect personal or corporate data against the unsolicited access of third, possibly hostile parties, namely hackers, data thieves and other digital fraudsters. But due to the viscosity of the legal system, decades have been wasted in an unregulated, “wild West” environment. For example, while hacking was an issue already in the early 1980s, the first legal act against hacking was passed not earlier than 1990, the Computer Misuse Act (CMA) (Murray, 2016). The problem of timely regulation is more common than expected.

In general, new technologies tend to confront legal systems with difficult questions that often interfere with traditional notions of how things should be regulated. Social values and morality are constantly challenged by this ever-altering ecosystem of innovations whose vast applications call for novel approaches that must be developed in order to preserve stability within society, the economy, and politics. This is of course time-consuming and makes myriad abusive acts possible during this unregulated phase. Worryingly, any crimes that occur in such a time of transition won’t be punished at all, since there is no specific law against them. Counterintuitively, the gap between technological state of the art and legal regulation will only grow with modern tech innovations.

As of now, the legal framework represents the most effective way of regulating these social dynamics influenced by – among other things – generally accepted values, rebellious opinions of various social groups, new incentives from different cultural backgrounds, and uncertainty caused by a lack of knowledge. Concerning the relationship between the law and innovative, often disruptive technologies, the law can be considered as “a method of technological risk management and plays a constantly increasing role in that regard” (Pöysti, 2004). With regard to the identified interaction, a proposal will be made in the conclusion to manage the risks posed by the technology (ibid.).

More often than not, legal regulation does not prevent undesirable acts in cases of innovative technologies but gets established as a reaction to new crimes that are only possible due to said technology. A prominent example is “hacking.” Conducting hacking activity against a company or a person without their permission is viewed as an offense under the Computer Misuse Act 1990 “unauthorised access to computer material” (ibid.). The Computer Misuse Act is one of the primary pieces of legislation that covers hacking offences, along with other legislation such as the Data Protection Act 2018 (ibid.).

Almost three decades separate both legal adaptations, which shows how slowly the legal systems react to technological challenges.

Clearly, hacking has been around at least since the 1980s. However, there was no legal framework to punish hacking activities until 1990; in fact, the Computer Misuse Act had to define the legally relevant act of hacking. And to define data protection took the US government until 2018!

### Data Protection in Europe and the US

In Europe, the European Union installed the DSGVO (Datenschutzgrundverordnung, engl. General Data Protection Regulation, GDPR) back in 2016 as a complex legal act to unify the rules for the processing of personally relevant data on an EU-wide level. With the DSGVO being quite restrictive, this resulted in a lot of legal issues regarding the international exchange of data, in particular in terms of the United States. In the US, the data protection standards are quite different and depend on the companies and their goodwill for transparency. However, to be able to move data from the US to Europe, the data quality had to be enhanced on the US side. But, in fact, the issue is already much older.

**Safe Harbor Agreement**

This was an attempt to regulate data transfers between the US and Europe. The act was active between 2000 and 2015, and was followed by the Privacy Shield framework.

Remarkably, the DSGVO evolved from a legal framework from 1995; the EU directive was designed to protect natural persons in the event of personal data processing and/or distribution (Arning et al., 2021). The issue was already pressing in the early 2000s. Since then there have been initiatives like the **Safe Harbor Agreement** and the Privacy Shield framework, agreements which force companies to obey to certain data quality standards (ibid.). Only then they can make their data accessible for European companies. Most notably, the safe harbor agreement was rendered incompatible by decision of the European Court in 2015, following the arguments of Austrian data protection activist Maximillian Schrems (ibid.).

To fill the gap, the Privacy Shield Agreement was fostered. However, no real commitment was put into the further adaptation of the US legal system, and realizing the same issues still persisted under a new umbrella, activist Schrems once again went to court – and won (ibid.). The European Court rendered the privacy shield as violating the standards of DSGVO, which put an end to legally binding international data transfers, especially to US companies. Let’s consider Google Analytics as an example. Residing in Ireland, Google Analytics itself would not come under the Privacy Shield, since Ireland is part of the EU. However, since it exchanges data with Google US, it does fall under the Privacy Shield. Data transfer would be illegal in this case.

On the other hand, the big social media players like Facebook (now Meta), Instagram, or Tik Tok are known for routinely violating DSGVO standards. Facebook has a history of verdicts that punished the social media giant for violating European data protection standards. Admittedly, the DGSVO standards aren’t particularly suited for social media contexts and if taken literally, probably the lion’s share of all online postings would be illegal. To legally post a picture of, let’s say, a birthday party, it would require the written declaration of consent to use the picture, signed by everyone in the photograph. These in some regards over-strict aspects of the DSGVO are subject to optimization in order to make it more practical.

The „safe harbor” agreement was an attempt to regulate data transfers between the US and Europe. The act was active between 2000 and 2015, followed by the „privacy shield” ac

Regarding these persisting issues, a call for a unifying solution that is binding for each and every international participant seems to be inevitable. National or even federal deviations in data protection standards are unacceptable; even continental differences should ideally not be tolerated. One global data protection law that avoids the mistakes of its predecessors should be the mutual goal. And computer science with all its interdisciplinary efforts can contribute a great deal to the evolution of such a solution.

### Data spying, Cyber spying, and Cyber espionage

Data spying, sometimes also referred to as cyber spying or cyber espionage, is characterized as intruding into private or enterprise hard drives or servers with the goal of obtaining specific data. The software tools used for this act of espionage are usually proxy servers, code cracking methods, and spyware. In contrast to simple hacking, in the context of cyber spying there is often much more crucial data at stake. Possibly classified information, compromising images, or data of political weight make the act of data spying even more dangerous. Sometimes the hackers are single perpetrators, but often they are organized into hacker groups. Some of them are altruistic by claim, like “Anonymous,” while others are rather shady and obscure. Russian hacker group “Cozy Bear,” classified by the US government as an **advanced persistent** **threat**, is associated with ties to several intelligence services in Russia (Alperovitch, 2016).

**Advanced persistent threat**

An orchestrated, long-term attack on a network, regularly perpetrated by a well-educated attacker assigned by a government

The “cyber army,” a huge group of Russian hackers, attacks certain online discussions to alter the course of conversations and implement their political agenda. Cyber spying has now also expanded to the monitoring of the activities of public sites like Facebook. The most basic characteristic is surely its tendency to be intentionally malevolent; it is either executed to harm or to generate profitable information. Cyber spying is thus to be seen in a bigger context as a strategy to obtain particular goals, which may be political or economic.

One of the most well-known examples of a cyber spying assault took place back in 2009. After Google noticed a stream of attacks on selected Gmail accounts, the company reported the cyber-attack. When Google disclosed the attack, other prominent companies like Adobe and Yahoo confirmed to have been attacked in the same manner. The hackers used a vulnerability within Internet Explorer, and the issue has been addressed since.

### Self-study questions

1. What are the main differences of data protection in EU and US? (DSGVO: strict standards; US: despite the data protection act still not consistently regulated
2. Describe cyber spying in your own words (cyber spying or cyber espionage, is characterized as intruding into private or enterprise harddrives or servers with the goal to obtain specific data)

## 2.3 Long-Term Archiving

Another problem associated with data is the question of how it can be archived permanently so that future generations can also access it. The exponential growth in the volume of data worldwide means that most of the data that exists today was created only a few years ago. In order to make this data permanently accessible, various aspects must be taken into account. The first aspect is the storage medium used. Our knowledge about ancient civilizations is largely fed by the written sources they left behind. While inscriptions on stone blocks easily last for thousands of years (and manuscripts, for several hundred years), electronic media have a much shorter lifespan (see table). In addition, invaluable sources have been destroyed again and again in the course of history, either intentionally or accidentally, e.g., by fires (Library of Alexandria). The term *Long-Term Archiving (and Notary Service)* stems from cryptology and constitutes a major branch of the field of Digital Preservation (DP). Long-term archiving describes the process of generating and maintaining data that is stored for long-term availability. The Internet Engineering Task Force (IETF) established the working group “Long-Term Archiving and Notary Service,” which was active between 2003 and 2011. The working group developed specifications concerning the detectability and integrity of electronically stored documents. Its relevance comes into play in a vast variety of contexts, for instance, when users need to prove the existence and/or validity of electronically stored data over a virtually undetermined time span (Lorie, 2001). Given the importance of long-term data archiving, the issue of data storage comes into play. While huge servers constitute the foundation of most data-driven companies, cloud storage adds both computing power and storage volume for more short-term oriented applications.

Considering the demands of the particular project that is managed, it can surely make sense to store data in proprietary formats. However, this demands that the software that is needed to open the data is available during the whole project. To ensure the stored data can be opened in one or two decades from now, proprietary formats don’t make sense. Non-proprietary formats like csv are more likely to keep the data accessible in 20 years or more.

The primary goal of any long-term archiving method is to secure proof of a record filed in an electronic document at some indefinite point in the future. Hence, long-term archiving must include all kinds of use cases, such as contracts, land deeds, medical records, criminal records, and wills. Examples of common long-term archiving contexts include the following (Lorie, 2001):

* A company stores contracts on a service provider’s system.
* A hospital stores medical records on an internal system.
* An individual wants to provide proof that they possessed a particular document at a particular time.
* A law enforcement officer wants to store criminal records in ways that ensure the integrity of the data for years, possibly decades.

Because of the long-term aspect, long-term archiving must take into consideration the fact that current techniques age and may not be available in the future. This applies to the storage media used, including formats such as Tagged Image File Format (TIFF) and now PDF/A, which are the contemporary standards but are likely to be replaced by others within 20 years (ibid.). Cryptographic algorithms that are used for signing documents might also be outdated in years or even decades.

|  |  |
| --- | --- |
| Life expectancy of storage media | |
| **Medium** | **Estimated duration** |
| Ceramic boards | Min. 5000 years |
| Stone tablets and stone paintings | Several millennia |
| Books and manuscripts on acid-free paper | Several centuries |
| Books and manuscripts on acidic paper (19th/20th century) | 70–100 years |
| Compact disc (CD) | Est. 50–80 years |
| Hard drive (during operation\_ | 2–10 years |
| Flash drive (stored) | 2–10 years |
| Magnetic tape | > 30 years |

With digital media, there is the added problem that not only must the medium survive, but there must also be a way to access it. In the first decades of digital technology, programs and data were stored on punched cards or floppy disks, which even today can only be read by a few computers. Therefore, the file format in which the information is stored must also be known and readable.

The question of how a digital long-term archive should be designed to circumvent these difficulties has been discussed in various ways. One approach is the Open Archival Information System (OAIS) standard for electronic archiving defined by the space agencies NASA and ESA. It is intended to preserve digital information and make it permanently available (Lavoie, 2004).

Another important aspect is the understanding of the content: Even if media can be read, it is not assured that their content can be read and understood by people in the future. While the oldest Chinese texts from the Bronze Age (ca. 1500 BCE) can still be understood today (Hart-Davis, 2015, p. 61), written documents from other early advanced civilizations such as the Bronze Age Indus culture (ca. 2600–1900 BCE) have survived, but they cannot be deciphered because the language has been lost (Hart-Davis, 2015, p. 59).

A practical example of why the intelligible storage of messages over long periods of time may be needed is provided by the construction of nuclear waste repositories. These are estimated to be lethal for several 100,000 years – longer than our species has existed (Piesing, 2020). Proposals for warnings aim at a combination of texts (in special rooms on the site and in archives around the world) and physical features such as stone pillars (ibid.).

### Self-check questions:

1. Please mark the correct statements.

* Texts produced by humans can be accessible after millenia. (R)
* Digital storages can be read out after 100 years without a problem. (W)

## Summary

With the ongoing digitization and networking of all areas of business and private life, data is accumulating in ever greater quantities. New technologies such as big data make it possible to collect this data and evaluate it in real time. Systems that use artificial intelligence (AI) draw conclusions from it independently. Personal data is a lucrative business for companies and of great interest to states. Its protection is regulated in Europe by the General Data Protection Regulation (GDPR). Archiving data for future generations presents a significant technical and cultural challenge.

# Unit 3 – Economic Impact of the Information Society

**Study Goals**

On completion of this unit, you will be able to …

... define the economic significance of information society.

... explain how the mechanisms of globalization and monopolization have intensified in the information society.

... discuss the strengths and challenges of the Open movement.

... identify the effects of digitalization on the labor market.

... critically discuss the mechanisms for the protection of intellectual property.

# 3. Economic Impact of the Information Society

## Introduction

The digital transformation that characterizes the information society is the leading force of incrementally (and in some cases even exponentially) rising profits. The countries that are the most advanced regarding digitization derive a surplus of 20 percent compared to the late adopters. The data-driven economy is not only welcomed as a force that can counter the negative economic impacts of the COVID-19 crisis. Few studies evaluated the role of digital economy on the economic growth of countries along the **Belt and Road Initiative** and the impact of COVID-19 on their digital industries. (Zhang et al, 2022) As expected, the digital economy not only showed a positive effect on the economic growth. It turned out that COVID-19 has generally boosted the demand for digital industries, with the impact from the demand side being much larger than that from the supply side. (ibid.)

**The Belt and Road Initiative**

Formerly known as “One Belt One Road,” this is a global infrastructure strategy by the Chinese government. (“Belt and Road Intiative,” World Bank Archive, 2019) It was founded in 2013 as an orchestrated investment in almost 150 countries. It´s aim to foster trade relations evokes notions of a modern silk road.

Digitization is generally associated with less unemployment, more cost efficiency and substantially higher profits. (Lee/Chen, 2021) Enterprises and start-ups make use of state-of-the-art technology, while other companies hesitate to implement digital innovations and join the mutual transformation process. This is mainly due to a large insecurity which innovations really suit the needs of the company. To distinct such useful innovations from buzzword-driven activism is a challenge posed to almost any employee on management level.

On the other hand, it showed that late adopters and elderly people tend to be marginalized in the growing information society. (ibid.) Hence, the skewed leverage of digitization clearly refers to age. Digitization seems to prefer the younger while punish the elder. This effect can be countered by education programs, but due to the ever-increasing speed of innovations, it will still overwhelm digital immigrants eventually. As a consequence, these parts of the population won’t be involved in the ways the digital world evolves and changes, with the result of reduced participation and increased marginalization.

Automation already rendered many of the simpler, highly repetitive jobs obsolete, while also high-skilled professions like radiologists or law specialists are at stake to be automated. Kai-Fu Lee estimated in his bestselling book „AI superpowers” that up to 40 % of all jobs are automated by the year 2033. (Lee, 2018) This is possible due to the crucial role of pattern recognition; AI systems can detect specific patterns that indicate cancer or a hidden flaw in some legal act much more reliably than any human being. But these systems can only evolve because they are enabled for constant learning.

On the other hand, new professions will emerge. But it’s highly doubtful that these professions will be attainable by the truckdrivers, factory workers or food deliverers whose jobs have been eradicated by automation. An unconditional basic income might soften the threatening social unrests that could result from relentless waves of automation; yet it is unclear how to implement a basic income while still keeping people in the working market. (Lee/Chen, 2021, Lee, 2018)

A basic income seems only to make sense if it allows for a substantial buying force. Only if enough individuals can afford to buy products, the industries are able to ensure organic growth. Any basic income should not allow a hedonistic lifestyle of Romanian decadence though, as a broad and versatile economy cannot survive on the wealthy alone. No basic income should foster laziness and Bohemian satisfaction. Hence, incentives could motivate hidden talents to let their gifts blossom and encourage them to create music, books, art, or movies. By incentivizing creativity and punishing a passive consumer’s attitude, the creation of human culture could blossom and evolve to new levels. As a matter of fact, these issues need to be tackled and regulated better sooner than later, and ethics commissions are invited to invest their energy into the solution of these pressing societal issues.

The companies that the information society has spawned represent a significant economic factor. The industry association Bitkom estimates the German market for IT, telecommunications and consumer electronics at 174.4 billion euros in 2021, with over 1.2 million people employed in these sectors in Germany (Bitkom e.V., 2021). Worldwide, the sector turns over more than $5 trillion a year (Statista & IDC, 2021a) and employs more than 55 million people (Statista & IDC, 2021b). The information society has also created many new opportunities for access to information (e.g., the global online encyclopedia Wikipedia), communication (e.g., free worldwide videoconferencing), and economic activity (e.g., online commerce, easier access to market information). In addition, however, there are economic effects of the information society that society must critically monitor, e.g., with regard to monopoly formation, changes in the labor market, and intellectual property. What trends can be observed here? How do they differ from similar developments in economic history? And what possibilities are there for us as a society to accompany these developments critically and constructively?

## Globalization and Monopoly Formation in the Economy

### Globalization

The globalization of business and culture has been a defining phenomenon of the twentieth century. However, international trade had existed since antiquity and multinational corporations since at least the seventeenth century (e.g., the British East India Company). After World War II, much greater global interconnectedness began due to political alliances, growing trade, and favorable global transportation. Globalization is defined as “the intensification and acceleration of cross-border transactions with their simultaneous spatial expansion - or, more briefly, the compression of space and time” (Menzel, 2002)

It is clear that this “compression of space and time” would not have been possible without worldwide communication networks, and indeed these processes were further reinforced by the advent of the information society. This gave rise to some of the fastest growing companies in history, involved in telecommunications (AT&T), information technology (IBM), software (Microsoft) or Internet search (Google). On the one hand, the growth of these companies was encouraged by favorable circumstances and good management. On the other hand, they were and are under permanent pressure to grow in order to satisfy their shareholders (shareholder value).

Thus, Internet corporations have a strong motivation to get people who do not yet use the Internet to do so. This runs under buzzwords such as “the next billion Internet users” (English “the next billion”) (Crichton, 2019). Meta, the company that operates Facebook, describes its mission accordingly: “Meta’s mission is to give people the power to build community and bring the world closer together. Our products empower more than 3 billion people around the world to share ideas, offer support and make a difference” (Meta Platforms, 2022).

The spread of the Internet in developing countries has undeniably positive aspects. For example, farmers in African countries use smartphones to find out about fair prices for their produce and to receive warnings about bad weather (Jacob, 2018). On the other hand, this often creates closed systems that can lead to dependence on one provider and reinforce negative tendencies such as misinformation and aggression. In fact, in developing countries, Facebook is often seen as synonymous with the Internet (Malik, 2022).

As a result of globalization, there are further opportunities for all parties involved: for example, outsourcing work has become much easier - companies in industrialized nations can relocate work to developing countries, creating relatively good jobs there that offer new prospects for people (Miebach, 2020, p. 334). Conversely, jobs in the country of origin are potentially lost as a result, and people in industrialized countries are suddenly in competition with cheaper labor around the world. In addition, outsourcing is not always easy and cultural difficulties in cooperation have to be overcome.

Our modern world of global trade is a result of the export and import of good across borders. Globalization describes this process of exchanging material, technology, services, information and investments all across the globe. Ostentatively, the multi-layered effects of globalization are highly complex, sometimes hard to determine and often share a political dimension. The main drivers of the globalized economy are technology, transportation, and international cooperation. (Lee, 2018)

Trade across country borders is nothing new or innovative at all, since the exchange of goods has been around for centuries. The Chinese silk road is a prominent example of early global trade. Yet, without the technological infrastructure, this form of international trading remained an exception. Since the 19th century, the first forms of globalization were pioneered by steamships, railroads, and later on planes, but also by increasing economic cooperation across borders. (ibid.)

After the two world wars overshadowed the developing globalization, causing diametral effects, the United States started to create a global economic system governed by mutually accepted rules and overseen by multilateral institutions. (Lee, 2018) One of the most obvious benefits of globalization is the increased availability of goods for lower prices. This is due to the comparative advantage that stems from the very premise of globalization – each country should focus on what it produces best using the most efficient amount of resources. On the other hand, the effects of a growing global market are not always beneficial, especially for the low-wage workforce. According to a study by Autor, Dorn et al., lower-wage manufacturing workers within industries that faced import competition experienced substantial earnings losses, while higher-wage workers relocated to companies outside manufacturing. (Autor et al, 2018) A similar tendency already showed in the context of automation. Not every painter can become an avid painting drone pilot, and not every store manager can evolve himself into a VR designer. And in both cases, globalization and automation, the low-wage workforce has virtually no leverage to improve its situation, since there is a high supply of resources in this segment of income and the robots are already starting to take over many low-skill-level jobs.

At the other end of the spectrum, the formation of monopolies goes on and makes it even harder for the blue-collar resources to secure a living. Global players like Amazon are not only known for the huge profits they generate, but also notorious for their relentless work culture that is often compared to a form of modern slavery. Most precariously, the pressure of automation forces non and low qualified workers to accept ever-decreasing wages. This is because a growing pool of unemployed will fight for ever less fitting job descriptions. (Lee, Chen, 2021) Many of the market economy’s own mechanisms of self correction, as postulated by Adam Smith (for example the assumption that high unemployment will push down wages, which forces the prices to also lower to a point where consume is setting in again, incubating the economy) will not work in an AI driven society. (Lee, Chen, 2021)

However, despite worldwide waves of start-ups, market power is concentrated on a few providers in the USA (GAFAM: Google, Amazon, Facebook, Apple, Microsoft) and China (BAT: Baidu, Alibaba, Tencent) due to digital network effects. (Rusche / Lierfeld, 2022) The ever-increasing volume of data that the successful monopolists can use gives them an unassailable competitive position, especially since data concentration promotes a parallel concentration of capital. They are not only innovators, but also reorganizers of well-known and successful business models. An iconic example is Instagram, a social medium that is basically just an optimization of specific Facebook functions: editing and uploading videos and sharing photos that can be easily and quickly edited with filters. Consequently, Instagram was bought up by its big competitor and digital monopolist Facebook, admittedly for a sum - albeit low - in the billions. (ibid.)

The CEOs of the big data suckers are seldom significantly older than the target group of intended users, a circumstance that is likely to contribute to the success of their companies. What makes a company fit for the future in times of perpetual upheaval beyond this cultural factor? (ibid.)

As we know, Alibaba, the world’s largest retailer, doesn’t own any ware, AirBnB, the largest accommodation provider, doesn’t own any hotel beds, and Uber, the largest cab company, doesn’t own any cars. The success of these game-changing companies lies in the added value they create: they are able to make a known service cheaper, more convenient, faster and easier to provide by optimizing business processes through continuous analysis of consumer data.

Lee and Chen envision a future where global energy supply is mainly maintained through sustainable energy sources. This, of course, would alter the global economy, even making third world countries possibly competitive due to the gain of independency. When the costs for material, energy, and production fall with historical unparalleled velocity, mankind is entering the stage of abundance. (Lee/Chen, 2021) The think tank RethinkX estimates that, given a 2 billion dollar investment, energy costs in the US could be as low as 3 cents per Kilowatt hour – a fourth of the current price. (ibid.)

However, contemporary politics point into a diametral different direction, as a veritable energy crisis is emerging. This shows that any anticipations of the future rely on the maintainance and stability of basic trajectories in the present. Unfortunately, it sometimes takes less than a year to render studies outdated – which is about the same time it takes a study to publication. With the trend for sustainable energy sources unbroken, there is still hope to solve the energy problem in the near future, thus enabling for a new level of participation of marginalized countries and human resources.

To fight for more participation of marginalized regions and people isn’t only a humanitarian act; it is also rational because the demand for specialists despite automation is still unbroken. However, inequality rises in certain parts of the world whereas in other it is reduced to a minimum.

**Purchasing Power Parity**

The PPP is the measurement of prices in different countries that uses the prices of specific goods to compare the absolute purchasing power of the countries´ currencies. To an extend, the PPP is also a metric for people´s standard of living.

According to the World Inequality Report, the Middle East and North Africa is the most unequal region in the world, Europe has the lowest inequality levels. An average adult individual earns **Purchasing Power Parity** (PPP) € 16 700 (PPP$23,380) per year in 2021 whereas the average adult owns € 72,900 ($ 102,600) in general. (wir2022.wid.world) These averages mask wide disparities between and within countries. The richest 10% of the global population currently makes 52% of global incomes, whereas the poorest half of the population makes 8% of it. (ibid.) On average, an individual from the top 10% of the global income distribution earns €87,200 ($122,100) per year, whereas an individual from the poorest half of the global income distribution makes € 2,800 ($ 3,920) per year. (ibid.)

Global wealth inequalities are even more pronounced than income inequalities. The poorest half of the global population barely owns wealth: it owns just 2% of the total. By contrast, the richest 10% of the global population own 76% of all wealth. On average, the poorest half of the population owns PPP € 2,900 per adult, i.e. $ 4,100 and the top 10% own € 550,900 (or $ 771,300) on average. (ibid.)

Inequality varies significantly between the most equal region (Europe) and the most unequal region (the Middle East) of the world. In Europe, the top 10% income share is equal to around 36%, whereas in the Middle East it reaches 58%. (ibid.) In between these two bounds, a diversity of patterns are observed. In East Asia, the top 10% makes 43% of total income and in Latin America, 55%. (ibid.)

Surprisingly, the globalization degress declined slightly over the last decade. This has been revealed by the Globalization Report 2020. The extent of a country’s interdependence with the rest of the world is measured with an index that is very closely aligned with the established “**KOF Globalization Index**” of the Swiss Federal Institute of Technology in Zurich.

### Monopolies

If a company becomes too large in one or more markets, there is a risk of monopoly formation. Monopolies, i.e. markets in which only one supplier is active, are well-known phenomena in economic history. One notable monopoly was, for example, the British East India Company, which handled trade with the British colonies, especially on the Indian subcontinent, from the 17th century onward. In some cases, it owned lands there that were larger than the British national territory.

Monopolies are usually seen as detrimental to the market because the supplier (monopolist) can charge excessive prices and is less motivated to develop its products or services further (Bundeszentrale für politische Bildung, 2016). Therefore, states have established institutions to ensure competition and prevent monopolies. In Germany, the Federal Cartel Office is responsible for this. It has already issued fines in the hundreds of millions of euros in important cases involving price agreements in the cement industry and in the coffee trade. At the European level, the Directorate General for Competition, as part of the European Commission, monitors the markets and ensures fair and equitable competitive conditions.

Despite its open culture and democratic values, the digital world shows a strong tendency toward monopolies for several reasons:

* The growth pressure that companies are under has already been mentioned.
* In addition, it is usually easy and free to use online services such as search engines and social networks. Accordingly, online service providers - compared with manufacturers of consumer goods, for example - incur only very low additional costs per new user. in business administration, the costs incurred by producing an additional unit of quantity of a product or service are referred to as marginal costs. Accordingly, the business models of online companies have also been called “zero marginal cost business models” (Frank, 2018).
* The first company to enter a new market has a special advantage in the online world (first mover advantage). Due to the low costs, users are more likely to use the services of this company than those of possible competitors. The latter only have the chance to offer a much more convincing product or to try to buy out the “first mover.” This explains the considerable investments that large corporations have made to buy up comparatively new and small competitors, for example in the case of YouTube (acquired by Google in 2006 for $1.65 billion) or Instagram (acquired by Facebook in 2012 for $1 billion). Once such a network has reached a certain size, it continues to grow simply because users stay on the network to communicate with their contacts. This lock-in effect is one of the reasons why, despite considerable investment, no social network has yet been able to establish itself as an alternative to Facebook. On the other hand, we will see that such changes are possible in principle.

At present, it is becoming apparent that a few large American corporations (Google, Apple, Facebook, Amazon) increasingly control important platforms over which a large part of social life runs. Such monopolies are questionable from a societal perspective in several respects. In addition to the usual disadvantages of monopolies (in particular, less innovation and lower quality of products), there are here, among other things, higher risks of surveillance (since only a few companies hold very much data) and moral issues due to the increasing market power and political influence of such platforms (Stucke, 2018). Moreover, just like other global corporations, Internet corporations are adept at minimizing their tax payments so that the general public shares little of their profits (McHugh, 2021). How can states and civil society stop increasing monopolization?

Existing antitrust measures are applied fairly consistently, at least in Europe. The software company Microsoft has long been criticized for its dominant role in the market for operating systems and office applications. It also used aggressive methods to keep competitors at bay (e.g., non-compatible file formats or bundling the Internet Explorer browser with the Windows operating system). Over the years, it has been fined or fined heavily by European antitrust authorities on several occasions (European Commission, 2006). More recently, the EU Commission has repeatedly fined search engine operator Google billions of dollars for abusing its market power (Stucke, 2018). With the Digital Markets Act, a law that has been implemented in November 2022, the European Union wants to further regulate the market power of large Internet platforms: “One goal is that there should be more freedom of choice. For example, users should be able to decide for themselves which browser, which virtual assistant, which search engine they want to use” (Lindern, 2022). Similarly, interoperability between applications such as messaging\_platforms should be increased. Internationally, it has also happened that companies have been split up when their market position was too dominant. One example is the American Telephone and Telegraph Company (AT&T), which held a monopoly on the telephone network in the USA and Canada in the 20th century. In 1984, the corporation was split into seven regional companies.

The question of how state judicial and tax systems can deal with such international corporations has also not yet been resolved. Internet corporations offer their products and services worldwide, generating substantial profits. Nevertheless, there is often little or no tax in the countries where the profits are made, as taxes are dependent on production sites. In addition, there is the question of how intangible assets such as data and services should be taxed globally. The European call for a global digital tax to tax Internet corporations is being discussed and seems to lead at least to a global minimum tax for such corporations (Mayr, 2021). Finally, one aspect that should not be neglected is that users often have the freedom to switch to other providers at any time. Especially in the lucrative area of search engines, this has indeed already happened. In a trial about Google’s market power, then-CEO Eric Schmidt pointed out: Google’s own success reflects how dynamic and unpredictable the Internet can be. By 1998, Fortune declared that Yahoo! had “won” the competition for search engine users. Nevertheless, Google established itself as a major player by the early 2000s and surpassed Yahoo! in 2004. (The Power of Google, 2011)

Thus, the question of how to deal with monopoly formation lies not only with society, but also with individuals.

### Self-check questions

1. Please tick the correct statements:

* Globalization began in the 20th century. (W)
* Google had to pay a few hundred millions of dollars in fines in Europe. (W)
* Google had to pay billions of dollars in fines in Europe. (R)
* Globalization is merely a modern trend. (W)

2. Please complete:

The first company to occupy a new market is called a first mover.

The lock-in effect explains why social networks continue to grow on their own once they reach a certain size.

## Open Movement

The development of computer hardware and software in its early days was characterized by a spirit of openness and sharing. At the Homebrew Computer Club in Menlo Park, early IT hobbyists met to share their findings and support each other (Computer History Museum, 2022). This spirit lives on in the Open movement. Unlike commercial providers of closed software or online services, there is a large community of developers who create open software and distribute it largely for free. “Open” in this case means that the source code of the software is public and can be edited by anyone interested.

Similar principles are also used to create texts and content on the World Wide Web. Wikis are software that makes it possible to host websites in such a way that all visitors can edit them. On the one hand, they are used to share knowledge within organizations (Krcmar, 2015, p. 686). On the other hand, there are also a number of public wikis on the World Wide Web - the online encyclopedia Wikipedia is the best-known example. What these projects have in common is that the participants do not act out of financial interest, but in the interest of the commons: “The participant in the crowdsourcing project has, instead of financial incentives, the prospect of a long-term benefit in that he or she could profit from further development and, in addition, the satisfaction of having made a positive contribution to the community and implemented its values and norms” (Miebach, 2020, p. 63). The concept of commons became popular through the research of Nobel Prize winner Elinor Ostrom (2003).

Based on the consent collaboration of distributed specialists who all contribute to the successful accomplishment of a goal, open movement developments are public domain. In contrast to the open source movement, which focusses on software technology, the open movement strives to produce physical devices that enable for novel applications, for instance innovative watches, trackers and all kinds of wearables. The open movement aims to create innovations for the good of everyone. The emerging innovations aren’t corrupted by financial or political interests, hence a way to democratize technology.

A great deal of innovations has been fostered through the bound forces of numerous scientists who cooperated for the sake of mankind’s progress, without monetarization as motivator. For instance, Barrack Obama proclaimed back in 2011 the *Materials Genome Initiative*, a national project that aimed to double the innovation speed of materials science. (Lee, Chen, 2021) Over the last decade, this initiative has established a huge data bank which enables scientists to create materials from sole atoms. (ibid.) Some of these nano-based applications resemble more of science fiction than of science; however, this shows the tremendous progress that can result from open movement and open source endeavours.

Additionally, it shows that the line between open movement and open source is sometimes rather blurry. In this case, the open source research has led to the creation of physical devices. Hence, both movements possess mutual ties.

In contrast to the open movement, the open source movement focusses on the creation of software tools which are an industrial factor for long. The most influential open source software systems are (Koranne, 2011):

* Mozilla Firefox, a customizable internet browser and free open source software
* Libre.Office, a complete office suite that offers presentations, documents, spreadsheets and databases
* GIMP, a free photo editing tool that offers some of the features commercial competitors provide
* VLC Media Player, a multimedia player that can process video, media and audio data and also webcams and streams
* Linux, an operating system that is known for its user friendliness, security and customizability
* Blender, a 3D graphics and animation tool
* GNU Compiler Collection, a compilation tool for software development in the C, C++, Ada, Fortran and many other programming languages
* Python, a common programming and scripting language used by custom software developers
* PHP, a software development language that is used for creating website and other digital platforms
* Shotcut, a video editor that offers powerful features including audio and webcam capture, color, text, noise etc.

The sheer versatility of this Top 10 underlines the tremendous influence open source software has acquired by now. Due to their easy and cost-free application, open source tools in particular help start-ups and small companies who largely benefit from the offered services, being enabled to work with professional software yet avoiding the costs that regularly come with it.

Despite these disadvantages, open source software is popular and widespread. Many of the mentioned open source software tools, like Linux, Python and PHP, have become industrial standards, contributing to the success of industry 4.0 as a whole. This underlines the tremendous meaning of human collaboration which acts out globally to further ignite the digital economy. For further reading, the comprehensive *Handbook of Open Source Tools* by Sandeep Koranne is recommended.

### Self-check questions

Please tick the correct answers.

1. Open source software is more widespread and popular as commercial alternatives. (R)
2. Open source software is less secure than commercial alternatives. (W)

## Change in the Labor Market

Higher efficiency almost inevitably leads to higher profitability, which is why, in the context of automation, the question of its applications is not if, rather how and when. Thus, any automation technology that increases cost efficiency, optimizes decision-making or simplifies processes – while not being a priori unethical – will certainly be introduced to the market as soon as they become available. Concepts that challenge and rethink traditional business models have proven to be both successful and disruptive. In cases where an innovation competes with a traditional business model, it is often the degree of disruption that makes its success measurable.

Thanks to their accurate pattern recognition, AI expert systems are superior to humans in a wide range of tasks, from mindless repetitive tasks to demanding professional fields such as radiology or highly specialized legal professions. The threat of general automation thus affects virtually all occupations that rely in some way on repetitive patterns. Only a few professions are exempt for the time being; these include professions that require a special interpersonal relationship of trust (e.g., psychotherapist) or require a great deal of experience coupled with manual dexterity (e.g., physical therapist). Of course, new professions will emerge while others disappear forever. But it is doubtful that there will be as many new jobs as old ones that become obsolete. This inequality will most likely lead to a massive wave of unemployment.

The concept of unconditional basic income is a much-discussed approach to counteract the devastation threatened by the tsunami of unemployment that automation has already brought. Freed from the need to earn money even from uncomfortable jobs, an unconditional basic income could allow people to let their previously untapped talents blossom. Talented (but not professional) musicians, artists or writers would no longer waste their lives driving cabs, serving tables or cleaning cars, but would have the chance to perfect their craft. The 10,000 hours it takes to become a master in one’s craft could easily be invested in a life secured by an unconditional basic income.

On the other hand, blooming hedonism might kill any motivation for striving and competition once life is freed from its basic economic pressure to survive. People could become comfortable with their simple and unambitious lives, become lazy and leisurely, and even reach a stage of late Romanian decadence. In a way, the situation during the second Corona freeze in 2020/2021 appears as a kind of foreshadowing of the satiated but unsatisfied way of life that could be fostered by an unconditional basic income. More than half a year of permanent home office has resulted in a significant portion of the population becoming overweight, addicted to alcohol, and increasingly immobile due to a significant lack of physical activity and exercise. While obesity is a complex health issue that can be caused by a multitude of factors, the study by Jones used national surveys to show a possible link between the unhealthy habit. (Jones, 2022) Relative to the 2019 to prepandemic 2020 period, significantly higher average BMI (+0.6%, p<0.05, N=3,555,865) and obesity prevalence rates (+3%, p<0.05, N=3,555,865) were observed among U.S. adults during the COVID-19 pandemic. (Restrepo, 2022) Significantly higher rates of any exercise participation (+4.4%, p<0.01, N=3,607,272), average sleep hours in a 24-hour period (+1.5%, p<0.01, N=1,907,798), average alcoholic drink days in the past month (+2.7%, p<0.05, N=3,577,090), and lower rates of smoking at least some days (−4%, p<0.01, N=3,625,180) were also observed. (ibid.)

Remote work, home office, and video conferences became common place during the pandemic, in particular during both lockdown phases. This has been possible due to the many office jobs that can be done in front of a computer screen. Professions that rely on physically working with the clients, producing materials or processing them cannot benefit from those new work modalities. Virtually any other profession can, though. Even physicians offered online office hours. Remote education boomed, embarking to become the new standard model of modern learning. Studies show that home office workers tend to be more focused, more efficient and more capable than they are after driving to work every day. On the downside, the line between work and life grows even more blurry, and emails that are received outside the official work hours tend to be answered, with the result of constant availability. For the employer this is very beneficial, but for the employee this situation comes at high costs. As a matter of fact, the employee is doing constant overtime, which remains unpaid regularly. Recent studies also proved evidence why zoom meetings and virtual conferences don’t produce the same level of creativity as in-person meetings can generate. (Shockley et al, 2021) One particular study revealed that turning off the camera during Zoom meetings can boost creativity. (ibid.) This is mainly because of the strict visual focus upon the relatively small screen in front of the user. Intuitively, the transfer of energy can’t be compared to a vivid live discussion were participants stand up, move around, open the window, get a cup of coffee together etc. In a nutshell, the results of the studies seem to suggest that interpersonal contact, social rituals and human interaction are the driving forces behind creativity and the creation of new ideas. Hence, virtual meetings and online conferences surely have their merits, but they cannot entirely replace direct human interaction and cooperation.

The crucial question with regard to an unconditional basic income is: which fraction will be larger - the party of the talented who like to develop their skills and cultivate their craft, or the party of the contented who play highly immersive metaverse games all day long? Directly from this thought derives another question: should a basic income really be unconditional? Or would it be wiser to make payment contingent dependent on the productivity or creativity of an individual’s lifestyle to counter the danger of hedonism and decadence?

A factor that molds the changing working market is the revolution of the materials. The contemporary world is structered by dematerialization, as Peter Diamandis has coined it. Dematerialization is the age of obsolete physical devices; software and platform technologies like smartphones have taken over their operational fields. (Lee, Chen, 2021). All kinds of devices have been rendered obsolete, from radios, cameras and maps to CD players. The specialists that work in these fields need to adjust to this situation. However, the examples show that it seems difficult to find job alternatives in related areas.

Asimov’s robotic laws demanded that no robot does any harm to a human being. In the context of automation, the robots that supplant the human workforce surely cause harm to those human beings and subsequently to their respective families. But again, it shows how interpretable and perspective-dependent a deceivingly simple concept such as „harm” can turn out. What surely counts as harmful for the obsolete workforce will be regarded as desirable efficiency enhancement for the profiteurs of the disruptions caused by automation.

### Self-check questions

1. Please complete:

Not only low-skill jobs, but also highly specific professions are threatened by automation.

## Intellectual Property

Much like with data security, the protection of intellectual property is a crucial aspect of the information society and the data-driven economy. Within some contexts, like the formerly discussed open movement or open source movement, intellectual property is freed from its tight legal frame and the idea to which the property rights relate is freely available. In other cases, scientific articles for instance, the intellectual property rights are clearly possessed by the authors. Using parts of this kind of texts demands to quote the source properly, and while there are several differing methods which are all legitimate in their ways, one has to do it actually. Not choosing any of the many quoting options equals a violation of the writer’s intellectual property rights.

The ever-increasing speed of development regarding internet communication, for example on social media platforms, doesn’t seem to leave much room for intellectual property though. Zettabyte after zettabyte of content is constantly posted within the still growing realm of social media platforms, and most platforms allow for sharing the content not only on that particular platform, but on other platforms as well as messenger services, email accounts and many more. Within a culture where „sharing is caring” it is mandatory to distribute contents, and any strict interpretation of intellectual property rights would only get in the way of the very premise of sharing content on social media.

Internet intellectual property can be protected by encryption, use of watermarks, and use of legal notices. The global nature of internet communications makes the publishing of intellectual property easier. However, the internet also makes the stealing or abuse of [intellectual property rights](https://www.upcounsel.com/intellectual-property-rights) much easier compared to other means of communication.

Intellectual property protection is an old concept that has existed for centuries. Modern legal attempts to protect intellectual property started in 17th-century England with the passing of the Licensing Act. Subsequently, the concept spread to the rest of the world and many countries had [intellectual property protection](https://www.upcounsel.com/intellectual-property-protection) laws before the advent of the internet.

The internet, however, revolutionized the way intellectual property is distributed and has necessitated a change of approach to intellectual property protection. There are a number of benefits people can get from publishing intellectual property using the internet:

* **reduced costs:**Compared to other methods of communication, using the internet is relatively cheap. The rise of the internet has encouraged a new breed of publishers who have made a fortune without investing. For example, while publishing books and videos traditionally required the services of a company, there are a number of self-made YouTube stars and book authors who are self-publishing on the internet.
* **the speed of information movement:**The real-time nature with which news travels over the internet means intellectual property publishers who use the internet can get instant exposure.
* **global reach:**The fact that the internet reaches virtually every corner of the globe gives intellectual property publishers an opportunity to reach multitudes of people. For example, it is easy for an author to sell books over the internet to people all over the world. This was virtually impossible before the internet age.

There are also dangers of distributing intellectual property over the internet.

* **uneven laws:**Although people in various countries can generally access intellectual property over the internet from publishers from around the globe, [intellectual property laws](https://www.upcounsel.com/intellectual-property-law) in various countries differ radically. This means many people can infringe on the rights of an intellectual property owner legally in their countries. For example, many people have duplicated software made by U.S. companies without the possibility of facing any penalty because such activities are legal in their countries. Although the intellectual property laws of some countries are in line with U.S. laws, some people in those countries can steal the intellectual property of U.S. entities without consequences because the U.S. has no extradition treaties with such countries.
* **the ease of duplication:**Unlike other forms of media where duplication of intellectual property is hard and may require the services of an expert, digital copies of intellectual property [can easily be duplicated by anyone](https://www.upcounsel.com/intellectual-property-theft). It only takes a few computer-mouse clicks to download [copyrighted](https://www.upcounsel.com/copyright) music, videos, or text.

Trademarks are relevant to the Internet because of the registration of domain names. In the early phases of the development of the Internet, the registration of domain names was on a first come, first served basis. This led to cybersquatting, the practice of registering names of companies and later selling those names to the companies in question at a higher price.

This situation compelled the business sector to place the protection of trademarks at the centre of Internet governance reforms in the early years of the Web. When the Internet Corporation for Assigned Names and Numbers (ICANN) was created, the US government demanded that the organisation develop and implement a mechanism for the protection of trademarks in the field of domain names. Soon after its formation, ICANN introduced the [Universal Dispute Resolution Procedure](https://www.icann.org/resource/pages/help/dndr/udrp-en) (UDRP).

The UDRP is now the primary dispute resolution mechanism for domain names. It is followed by all ICANN-accredited registrars (entities through which individuals register domain names) in the case of generic top-level domains (gTLDs; e.g., .com, .org, .net, .ngo, .blog, etc.) and some operators of country code top-level domains (ccTLDs; such as .tv for Tuvalu and .ws for Samoa). In brief, the UDRP specifies that most types of trademark-based domain name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name.

Since software and data can be reproduced without restriction, new challenges for intellectual property arise here. Especially in the early phase of the Internet, illegal distribution of music files, for example, was widespread. Out of the Open movement, demands have arisen for more extensive rights to make copies for private use. In the meantime, subscription models such as Spotify have become established here, enabling artists to earn at least some income (Schallmo et al., 2021, p. 592). Spotify would like to enable one million artists to make a living from the income generated by the platform - a goal that is apparently not realistic in the long term (Ingham, 2020).

The question of the extent to which software is subject to copyright protection, e.g. through patents, is the subject of intense debate. Since patent law was originally created for technical inventions, it is unclear to what extent it applies here. According to German and European practice, a computer-implemented invention is patentable if it makes a technical contribution. The problem is that, in contrast to mechanical inventions, it is difficult to define what this contribution is. If patents are formulated too generally, there is a risk that they will prevent the future development of software in other areas as well. On the other hand, industry demands some protection for software innovations (Bitkom e.V., 2013). A famous example of a software patent is the PageRank algorithm (Brin & Page, 1998), the basis for ranking search results in the Google search engine and its early success in the market. This was registered to Stanford University because Google was developed there as a project as part of its founders’ doctoral studies. Google later bought the patent for shares in the company, which Stanford eventually sold for $336 million.

### Self-check questions

1. Why does it make sense to protect the intellectual property of technical inventions?

Companies would seldom shoulder the necessary investments if they did not have a certain degree of security that they would be able to profit from their innovations in the event of success.

2. What is the danger of granting patents on software?

It is difficult to define what the technical contribution of software is. If patents are formulated too generally, there is a danger that they will prevent the future development of software.

## Summary

The effects of the information society on the economy are massive. So far, they have been largely positive, at least in highly developed industrialized nations. But that could change quickly if jobs are actually lost to the predicted extent as a result of digitization.

Digitization has also spawned a small number of companies that operate globally, have some of the highest revenues in history, and often hold monopoly-like positions in their respective fields. They provide considerable wealth. Nevertheless, societies must take care to protect free competition and ensure that prosperity also benefits the general public. In this context, the Open movement is noteworthy, which has created remarkable projects without much economic motivation.

From the perspective of developing countries, the information society has also had a positive impact, creating relatively well-paid jobs in IT and outsourcing. At the same time, the question is whether this is enough to contribute to an equalization of living conditions. Negative effects, such as the poor working conditions of gig workers, are more noticeable where there are less strongly developed constitutional states and protective rights for workers. In addition, measures such as patent protection for medicines have a particularly negative impact in less prosperous countries.

# Unit 4 – Social Impacts of the Information Society

**Study Goals**

On completion of this unit, you will be able to …

... describe the social impact of social networks.

... name the possibilities of surveillance in the digital space.

... identify the opportunities and risks of the digitization of education.

... explain the importance of inclusion and diversity in computer science.

... discuss the role of computer science in relation to sustainability.

# 4. Social Impacts of the Information Society

## Introduction

The information society and information technology have had a variety of effects on society. Social networking sites, originally intended to strengthen contact between acquaintances, now influence political life in many countries and can deepen social divisions. The possibilities for monitoring individuals are almost unlimited, and governments sometimes exploit this to persecute their critics instead of protecting the freedom of their citizens. At the same time, digitization offers undeniable opportunities, for example, to offer many more people access to education than ever before. Diversity is increasingly important. While computer science has been decisively shaped by women from the beginning, today it is often perceived as male – and this is reflected in the systems that computer scientists create and that we deal with every day. If nothing else, digital systems can help us reduce humanity’s CO2 emissions and slow the climate catastrophe – or they can accelerate it. The decision is up to society.

## 4.1 Social Networks

In the modern-day information society every citizen is embedded in a network of digital devices, applications, and ultimately decisions. Even people who avoid any digital identity or communication are involved in the decision making of machines. ADM, algorithmic decision making, is determining health insurance fees, evaluating job applications and interferes with many more layers of everyday life. This unparalleled accessibility of ADM for human affairs is mainly possible due to the digital duplication of each citizen.

As Hemel has put it, every single person exists as a „threefold person”: as physical being (persona 1), as digital extended person (persona 2), and as digital virtual person (persona 3) that basically consists of the distributed traces of data left behind by persona 1 and 2. (Hemel, 2021) Intriguingly, even digitally abstinent people are represented as digital virtual persons (persona 3), since they inevitably have left behind some traces of data. But the overwhelming majority of the population is indeed a threefold representation, hence consisting of one biological being and two digital personas. Regarding the enormous number of 4,48 billion of social media users worldwide (Woodward, 2022), its result is stunning: since every digital represented person exists threefold, the world is in the historically unique situation that the sum of these digital personas exceeds the number of existing real people. In fact, 13,5 billion digital citizen personas are almost double the world population!

**Weapons of math destruction**

These are models, tools and algorithms that decide over the course of people´s lives with pure mathematical and statistical logic.

While the benefits of the data-driven society we know today are known, analyzed and elaborated, its downsides are much more opaque and uncertain. Only now we realize the scope of the hazardous impact of what mathematician Cathy O’Neil calls **weapons of math destruction** (WMDs). Almost traditionally, WMDs act to the disadvantage of blue-collar workers while benefiting the white-collar workforce. These WMDs can be realized in a variety of instantiations which show varying degrees of complexity and ranging from low-tech to high-tech. For instance, a teacher test coined IMPACT was implemented in 2009 with the aim to evaluate the performance of the teachers. At the end of the 2009–2010 school year the district fired all the teachers whose scores put them in the bottom 2 percent (O’Neil, 2016, p. 4). At the end of the following year, another 5 percent, or 206 teachers, were booted out. (ibid.) The problem was that the impact test was blind to personal qualities of individual teachers, deeming some of the most popular and capable teachers as sub-standard.

Such undesired and ultimately unethical outcomes can occur when the system blindly relies on the validity of the test results. While common sense or general rationality is generally attainable for most people, it’s not implemented at all in algorithms. Pending further training, algorithms need to learn more about the “conditio humana” in general and about the individuality of specific subjects in particular. As of now and the foreseeable future, society needs to make sure that human decision makers remain in the evaluation process to avoid catastrophic misjudgments, marginalizations, and biases.

### Social Media

With the advent of social media, an entirely new class of communication models evolved. After the inception of Facebook in 2004, one of the very first well-known competitive platforms was the German-based StudiVZ (founded in 2005). Yet it quickly showed that Facebook had a better set of functions, but also a bigger vision than its competitors, eventually evolving into a multi-layer enterprise engaging in AI research. More specialized social media platforms emerged soon: YouTube, focussing on audiovisual content, started in 2005, Instagram simplified editing and uploading videos and pictures in 2010, Snapchat offered to post edited pictures that are only a few seconds available in 2011, and in 2016 TikTok went on to enable for selfmade lip sync music videos. All these platforms also work as social media platforms with instant messenger functions.

As of 2022, 56,8 % of the world’s total population is active on social media, which equates to about 4,48 billion people that use social media worldwide. (Woodward, 2022)

The total number of social media users is even higher, with an astonishing 4,62 billion users, equaling 58,4 % of the world population (Chaffey, 2023). What also comes to mind is that the total number of internet users isn’t significantly higher than the total of social media users. Remarkably, the number of unique mobile phone users is roughly 350 million people larger than the total number of internet users. However, both of these statistics are looking at eligible audiences aged 13 years and above. (ibid.) It is estimated that more than half of the children aged 11 and 12 have personal social media profiles even though most social media platforms have a minimum age requirement of 13+ years old. (ibid.)

The total number of global social media users increased more than threefold within a decade, as the following graphic illustrates. Remarkably, the gains didn’t significantly go down, as it is regularly the case with late adopters. A plus of 10,1 % between January 2021 and January 2022 shows evidence of the unbroken run on social media, suggesting that a large portion of these new users are children (Kemp, 2023). This is highly problematic, not only due to the fact that a great deal of these children will be below the minimum age requirement, but also due to the widely unknown longterm effects of heavy social media usage.

Depending on the features a specific platform provides, the gender demography varies tangibly (Beveridge, Lauron, 2023):

|  |  |  |
| --- | --- | --- |
| Gender demography across social media platforms | | |
|  | **Female User (%)** | **Male User (%)** |
| Snapchat | 60 | 40 |
| Pinterest | 78 | 22 |
| Instagram | 57 | 43 |
| Facebook | 44 | 56 |
| Twitter | 32 | 68 |
| LinkedIn | 49 | 51 |
| TikTok | 59 | 41 |
| YouTube | 45 | 55 |

The impact of social media is merely started to be discussed, and scientific studies are still rare. However, one of the first clear conclusions is the addictive potential of social media, in particular for the youth. Likes and shares are like tokens that result in physical adaptations; the human brain releases dopamin, initiated by the digital interactions. Ironically, it shows that the brain doesn’t seem to differ between a positive stimulus that stems from direct human interaction and from a digital one. This makes social media so addictive. (Spitzer, 2012) Of course, abusive, self-harming behavior isn’t restricted to social networks though; *problematic internet use* (abbr. PIU) or pathological internet use is categorized under the term **internet addiction disorder** (IAD; Chen et. al, 2003).

**Internet addiction disorder**

IAD is diagnosed in people who cannot control their Internet use without drugs and whose Internet use induces social and psychological dysfunction.

In particular, young people have been identified as the major risk group for developing PIU or even IAD. (Tomczyk, Solecki, 2019) According to a 2016 study conducted in Poland, 5,88 % of the observed students showed full-fletched internet PIU. (ibid.) Furthermore, PIU is connected with negative emotions offline (mostly boredom and a lack of self-control) and too little time spent on developing passions and interests. (ibid.) Tomczyk and Solecki locate a large portion of the responsibility to alter this status quo within the basic educational system. Failure to provide effective media education (focused on strengthening self-control when using new media) and neglecting individual passions and interests intensify PIU.

By 2022, this tendency has ramped up to an enormous 323 million estimated social media addicts. (Toth-Kiraly et al, 2020) And this number isn’t surprising, not even at first sight, since the most popular social networks are the ones who establish the addiction of their customers through the very design of the platform. Forstering general activity, interaction, and frequent content creation, social networks like TikTok make a billion dollar business case out of the insecurities and anxieties of some of the most vulnerable parts of society: children and teenagers. Statistics are concerning, to say the least. There even seems to be a correlation between the total daily time spent on social media and the suicide probability. Although it would be interesting to further differentiate through the spectrum of platforms, the sheer possibility to result in suicide is a disheartening, but even more relevant reality of social media usage. A recent study by Istvan Toth-Kiraly focuses on PIU’s effects on adolescents. The paper regards data gathered by a longitudial study of 1.750 high school students in Helsinki; the students are observed for a time period of three years. (ibid.) Toth-Kiraly states: „We think that PIU and depressive symptoms are likely to be co-occuring instead of one determining the other. They likely reinforce one another over time.” (ibid.)

Another study conducted by Yu et. al. examined the correlation between PIU and abnormalities of the EEG. The study analyzed the effect of excessive Internet use on the time-frequency characteristics of the electroencephalogram by wavelet transformed and non-negative matrix factorization (NMF), a new method that has been widely used in image processing and EEG signal processing. This study suggests physiological adaptations towards the incoming stimuli provided through the addictive behavior. Social media addiction statistics reveal 15 % of people aged 23-38 admit they are addicted to social media. The percentage of people feeling somewhat addicted to social media is highest at 40 % among those aged 18-22 and 37 % among people between 23 and 38. Then, 9 % of people between the ages of 39 and 54 feel they are addicted. (Woodward, 2019)

By far not only cyber mobbing, shit storms and bashmobs are the driving forces behind the epidemic depression and the tragic suicide deaths. The narcissistic and hedonistic, often totally fabricated perfect life that is portrayed by a great deal of successful influencers needs to be debunked as what it is: a commercial presentation that has nothing to do with reality. Furthermore, a large portion of the presented content isn’t real. In an interview from 2018, AI writer Yvonne Hofstetter was asked the following question: „Social bots lead the famous Turing test ad absurdum. Do we need new testing methods to be able to decide whether an information stems from a biological or artificial intelligence, or is this already a lost battle?” Hofstetter answered: „People have to know that 60 percent of the content available in the Internet is generated. The key word here is *digital literacy*. […] We are threatened by a profound confusion, a separation into fake news and official reports. Critical thinking is facing historical challenges here.” (Lierfeld, 2019)

Digital literacy must include the right amount of critical thinking and mental maturity to dismantle the virtuality of all these iconic lifestyle role models promoted on social media. In order to do so people must be further encouraged to speak openly about depression and to actively seek for help. Also the peer groups, friends and family need to be educated to watch out for suicidal warning signs. Even though there are already depression and suicide related campaigns, the awareness of the connection to social media use must be created. Scientifically, these are new psychological pathologies, evolved from use of technology, and the whole educational system has to react to their emergence. Teachers cannot advertise for the use of digital technology without admitting its potential downsides and hazards.

The values that are popularized through the different platforms are also a matter of concern. Instagram, for instance, is known as a realm where narcissism can blossom the most. Influencers and even Instagram models alter their pictures by using apps like Photoshop to make them look perfect in the desired ways. Insecure and immature parts of the youth tend to try to be like those perfect idols, while ignoring the fact that the icons themselves don’t look like portrayed on that platform. A veritable wave of teenagers, humbled and misled by their online idols, started to fight for their right for self-optimization in the most radical forms: plastic surgery, anabolic steroids, even body modification surgery. A rarely mentioned facet of digital literacy is surely the awareness about the most basic, mutual quality of all kinds of influencers: they influence. They are able to alter mindsets, belief systems, value canons, and even self models. A part of digital enlightenment is exactly this realization and the inevitable conclusion that forces the individual to reflect and rather choose accordingly to their own wishes and desires, not to that of a lifestyle agenda setting.

Regarding the ever-increasing average daily total screen time it appears as if is still unknown how hazardous these isolated, often almost solipsistic activities can become - for the social, mental, and psychological development of the children and teenagers who are exposed to excessive social media usage. The addictive (and hense destructive) potential of digital technology has been scientifically explored for more than 15 years. German neurologist Manfred Spitzer, for example, elaborated in his book “Digital Dementia” from 2012 how disruptive and malevolent the epidemic digital media addictions can manifest themselves in societies’ most valuable human resources: the youth. Beside diminished mental focus, distraction issues and many other undesired side effects Spitzer even describes neural adaptations that resemble dementia.

On the behavioral side Spitzer observes an increased recklessness in terms of mobbing and hate speech: The anonymity that has been established by digital media has tempted kids to act out offensive behavior they avoided earlier in fear of social control. (Spitzer, 2012) Spitzer supports his strong assumptions with studies by Sallet and Rushworth from Oxford Univerity; the group of scientists examined the relation between social ranking and social competence among rhesus apes (Macaca mulatta). In summary, the studies’ results show that living in a bigger group of individuals increases the social competence and stimulates growth in the areas of the brain that support social functioning. (ibid.) This increase of social competence results in an accordingly higher social ranking. The data from a study by Roy Pea and his co-workers suggests the conclusion that the usage of digital social media like facebook, which correlates with less real contacts, will lead to a reduced size of the brain regions associated with social functions, which inevitably leads to less social competence. (see Spitzer, 2012)

Cathy O’Neil regards the usage of the facebook algorithms as problematic and discusses as an example the huge uncertainty who of the many connected accounts will see a post that has been created. Of course, this issue stems from the company’s well-known data policy of gaining ownership of a post as soon as it is posted. „While Facebook may feel like a modern town square, the company determines, according to its own interests, what we see and learn on its social network. […] By tweaking its algorithm and modding the news we see, can Facebook game the political system?” (O’Neil, 2016)

Facebook researchers have been studying exactly the conditions whether their own platform can become politically influential. And indeed, the study showed evidence for this premise question. For instance, Facebook conducted experiments to hone a tool they called the „voter megaphone”. The idea was to encourage people to spead word that they voted. By this, Facebook built up social pressure to vote. In numbers, Facebook adressed more than sixty-one million Americans. By posting about people’s voting behavior, the platform instigated peer pressure. Studies have shown that the quiet satisfaction of carrying out a civic duty is less likely to move people than the possible judgments of friends and neighbors. (O’Neil, 2016) The underlying mechanisms are in principal well-known general societal issues; conformity results from people’s need to fit in. However, digital technology can amplify such issues due to their inherent scale-up abilities. Regarding O’Neil’s question, evidence emerged that social networks can alter the course of an election. Although the platform that added to, if not enabled Donald Trump’s successful presidential election in 2016 wasn’t Facebook, but Twitter, it showed that O’Neil’s question was all too righteous.

But the influence of social media easily crosses the skin-and-bone boundary, as constituted by the human skull. To put this into perspective – to overcome the skin-and-bone boundary is something the most advanced brain-computer interfaces aim for. While there are some successful implantations of interfaces that cross the skin-and-bone boundary, this is still rare and a tremendous achievement. Yet, digital technology in the form of social media platforms masters this task with ease. As recent studies revealed, the brain chemistry of heavy social media users is often altered and adapted towards the digital realm it is exposed to so regularly. Researchers hypothesize that since social media is easily accessible and competes for your attention with the promise of perpetual new content, heavy social media users become less able to ignore distraction in general. (Fotuhi, 2020) Not only does this lead to poorer cognitive performance, but it shrinks parts of the brain associated with maintaining attention. (ibid.) Obviously, technological influence can’t become much more visceral and basic than altering the human brain. Hence, there are writers who claim the advent of the age of the *homo digitalis* – a human being shaped, molded, and altered by the digital technology it is embedded in.

### Self-check questions

1. Who owns the content, once a user has posted in on a platform like Facebook?

The platform owns the content as soon as it is published / posted.

1. Is problematic internet use (PIU) an issue that spreads equally across the whole group of internet users?

No, since it affects rather the young.

## 4.2 Surveillance

Closely attached to, but not synomynous with cyber security, the issue of surveillance poses some similar questions about privacy, autonomy, and digital identity. All privacy-related issues are particularly precarious because of the many multidirectional influences and mutual interferences between the threefold digital personality. That being said, sensitive data leaked from persona 3 can cause undesired echoes for persona 1. But since persona 1 is the only sentient incarnation of the person, one could argue that only the information that is a direct hazard to the reputation or well-being of persona 1 is ethically relevant. However, this seems to represent a skewed view, since persona 1 and its digital emulation, persona 2, are that closely related that any digital affair which involves persona 2 will inevitably cause effects for persona 1. Usually, said effects are undesired; they can be as severe as an info hazard (see Unit 2.2)

A common argument that aims to apologize digital surveillance emerged during the post 9/11 terror crisis, when a great deal of surveillance methods was justified by the war on terrorism. The common reasoning assumed that just, honest people don’t have to hide anything, thus surveillance won’t harm them or violate their rights. But is the truth really that simple? Seemingly harmless data, for instance an event at the kindergarten or a reservation at a certain restaurant may cause real-world dangers, depending on the context. The information that a particular politician, for example, can be awaited at the event at the kindergarten or at a distinct time at the restaurant may be irrelevant for most people, but enables criminals to commit the very crime they were plotting against the hypothetical politician.

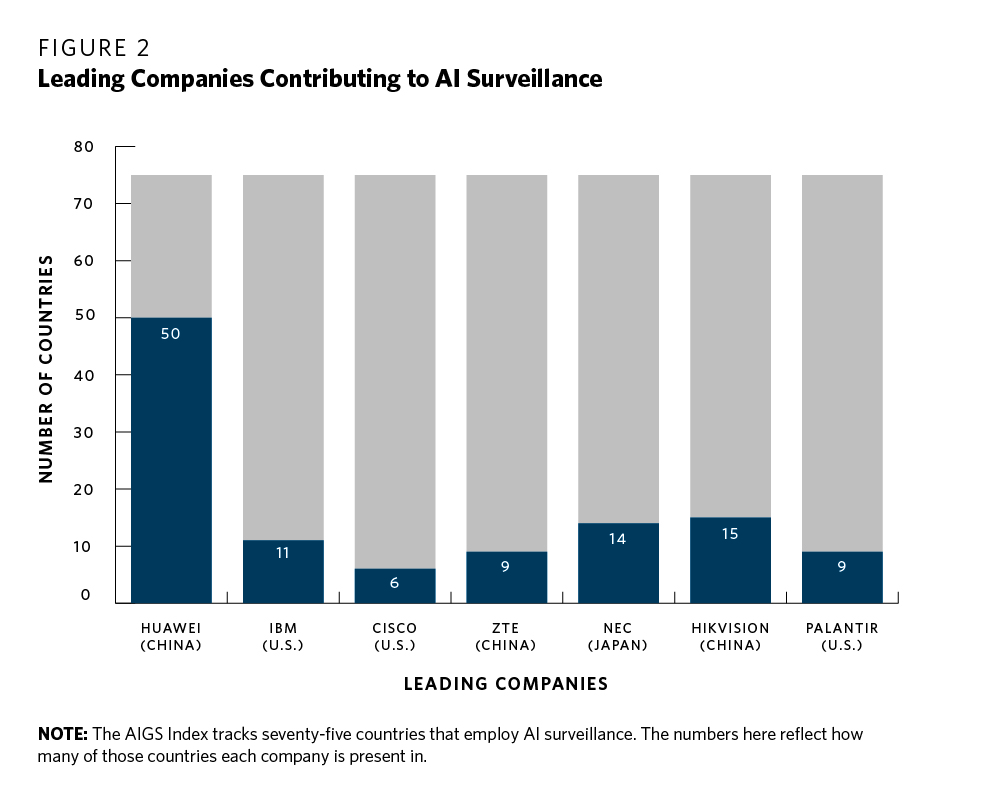
Some advocats of surveillance alter their initial argument in an attempt to relativize the threat – not everybody is a politician or general a person of interest. In stark contrast, most people focus on their private lives and avoid becoming public figures, so the argument goes. Yet again, the argument oversees some inevitable consequences of the information society. Common people work everyday to grow their reach in the digital realm, with the ultimate goal of stacking up millions of followers. Average folks strive to become influencers and role models to make a living by selling dreams. A substantial part of the population, from 6 year old tik tok stars to 60 year old fitness enthusiasts, engages in digital self-promotion, leaving behind traces of data in the process that could be problematic to a later time. Again, the danger lurks in the context of the situation. Bottom line is: the hazards of digital surveillance are not exclusively relevant for persons of interest, but essentially for all people who are embedded within some part of the digital realm. The awareness of surveillance and its manyfold issues should be a part of digital literacy as well.

A great deal of the job-threatening automation process has been enabled through some sort of surveillance technology. AI systems need to constantly learn from human behavioral data (for instance decision making conditions, process steps etc.) to be able to take over their tasks. The major technology that offers these almost omnipotent learning options is *robot-supported process automation* (abbr. RPA). An RPA is a software robot that is installed on the computers of the workforce, surveilling everything the resource does. (Lee, Chen, 2021) Through observing millions of people at work, the RPA systems learns how it can manage the workforce’s routine and repetitive jobs. (ibid.) The enterprise’s management will realize one day that it will be more cost-efficient when the robot completely takes over certain tasks from human beings. (ibid.)

Lee and Chen suggest to imagine a human resources unit with 100 employees. RPA could check the applicants’ curriculum vitae, define a pre selection and compare the applicants based on criteria in a job description. (ibid.) Given, there are 20 people working on this task, and RPA could enable them to evaluate applicants twice as efficiently. (ibid.) Hence, 10 human workers would become obsolete in this still conservative scenario. (ibid.) Regarding the learning speed of comtemporary AI systems, this ratio will soon be altered to the disadvantage of the human workforce. And all this has become not only possible, but also probable mainly due to one specific surveillance technology: RPA.

However, another and potentially much powerful surveillance technology has entered the market, and this is AI driven surveillance. A growing number of states are deploying advanced AI surveillance tools to monitor, track, and surveil citizens to accomplish a range of policy objectives—some lawful, others that violate human rights, and many of which fall into a murky middle ground. (Feldstein, 2019) Business harnesses AI capabilities to improve analytic processing; city officials tap AI to monitor traffic congestion and oversee smart energy metering (ibid.).

Leading Companies Contributing to AI surveillance

(Source: www.bankinfosecurity.com/adoption-ai-surveillance-echnology-surges-a-13101

Remarkably, China’s Huawei manages the surveillance of 50 other countries, while the US-america’s best effort by IBM counts only 11 countries. Regarding the rising relevance of cyber security and data protection, this skewed leverage shows how crucial it is to observe the competitors.

Feldstein’s AI Global Surveillance Index reveals some rather political background information about the involved parties. Liberal democracies are major users of AI surveillance. The index shows that 51 percent of advanced democracies deploy AI surveillance systems. In contrast, 37 percent of closed autocratic states, 41 percent of electoral autocratic/competitive autocratic states, and 41 percent of electoral democracies/illiberal democracies deploy AI surveillance technology.1 Governments in full democracies are deploying a range of surveillance technology, from safe city platforms to facial recognition cameras. This does not inevitably mean that democracies are abusing these systems. The most important factor determining whether governments will deploy this technology for repressive purposes is the quality of their governance.

Computer science has its own sub-branches to deal with the widespread, but at the same time pretty much clandestine influences of surveillance technology. A wide variety of studies analyze the societal, psychological and political effects of seemingly ever-increasing surveillance. The trade-off the information society has to face is no less existential than to decide how much freedom can be sacrified for the sake of increasing security. The complexity of the world, however, proves on a daily base how uncertain and unpredictable any anticipated outcome truly is. Ultimately, security can never be guaranteed, regardless how much freedom has been traded off. So is it really worth it?

Surveillance cameras, as an everyday example, have been implemented with the thought to possibly avoid the execution of crimes. As a matter of fact, CCTV surveillance came in handy to solve crime cases, but rarely to prevent them. This can be at least partly explained by the mostly rather spontaneous nature of crimes on the streets. That being said, the majority of these deeds isn’t rationally planned by the perpetrators. Thus, the rationale behind the CCTV surveillance fails – addressing rational minds doesn’t work with irrational perpetrators.

Modern surveillance technology enables for a seamless observation of subjects. Supported by intelligent algorithms and machine learning, the simultaneous surveillance of whole populations can be handled. The resulting vast streams of data can easily be filtered by whatever pattern an interested party is looking for, enabling for information about behavior, prejudices, preferences, addictions, passions, fears and many more. Popular and useful applications like Google maps, Uber or Tinder are all collecting information about the location and habits of the users. Even more, also behavioral data is collected and interpreted.

The inevitable streams of data each and any citizen emits can be of critical meaning in the context of federal institutions. In particular, the NSA (National Security Agency) is a household name for the ubiquitous surveillance carried out by governmental institutions. Surprisingly, still a majority (56%) of the US citizens regards NSA phone monitoring as acceptable, while a minority (45%) regards email monitoring at the hands of the NSA as acceptable. Since Facebook and its competitors are ultimately bound to obey governmental admissions, the logical conclusion is that everybody’s data can become involved in an official investigation, may it as a piece of evidence, may it as a tool to force for collaboration. Hence nobody is safe from the data-driven surveillance that is an inevitable consequence of the information society. As known by the medical context, there is no desired effect without undesired side effects. The same goes for the information society and in particular the data-collecting devices and applications that are so very characteristical for that particular societal epoch. All the blessings that enrich human life, make it safer and more comfortable come at a price. In the case of data-collecting digital helpers, it’s the threat of omnipresent surveillance and full transparency towards agencies that remain, although widely identifiable, largely opaque and unknown to the general public.

### Self-check questions

Please complete:

1. Surveillance technology is commonly justified by a trade-off between freedom and safety.
2. In the US, a majority regards phone monitoring as acceptable, while a minority accepts email monitoring.

## 4.3 Digitization of Education

In the wake of COVID-19, digitization of education has been progressed rapidly. The possibility to study remotely, without any need for personal contact, seemed promising during the COVID crisis, since it reduced or even eliminated entirely the necessity of meeting people in person, hence drastically reducing the risks of a Corona infection. However, the digitization of education has only accelerated through the COVID crisis; in principle, it has been around for more than a decade.

Given the many benefits of video learning and digital education in general, there is still a remarkable skew regarding the spread and regular use of digital technology in education. In order to appropriately address the effects of this technology, it is important to first understand where these tools are being deployed and how they are being used. Unfortunately, such information is scarce. To provide greater clarity, Feldstein (2019) presents an AI Global Surveillance (AIGS) Index – representing one of the first research efforts of its kind. The index compiles empirical data on AI surveillance use for 176 countries around the world. It does not distinguish between legitimate and unlawful uses of AI surveillance.

Novel technologies like digital learning assistants, virtual 3D worlds and Extended Reality create entirely new possibilities. (Miebach, 2020, S. 151–160). The internet has been created to make the cooperation between scientists easier. Hence, its growth early led to the hope of a democratization of educational contents, making them worldwide accessible. This has happened in a multitude of cases: reknown universities provide parts of their course as free online resource. (for instance OpenCourseWare of the Massachusetts Institute of Technology) and new competitors like the Khan Academy provide their own content for free. Beyond this, there are several free resources like Codecademy, which teach basic coding skills. Lastly, the internet offers learners access to the world’s knowledge, and additionally enables for discussions regarding related questions, for instance in social media groups or in communities.

Practically, it shows how hard even highly developed industry nations struggle in an attempt to combine traditional education with digital methods. Also the hope to foster properity in developing countries by free e-learning offers regularly fails. This is because the challenge istn’t only to create and provide the contents. The social context of the learners has to be regarded as well. Factors like the availability of essential hardware and the required user skills come into play here, but also issues like safe spaces where the learners can really focus and the evaluation whether they might be harrassed at work or in their marriage (Ndambakuwa & Brand, 2020).

### Schools online

The digitization of education remains a challenge also in industry nations. A lack of investments and know-how have slowed down progress substantially. All of that changed in March 2020, when contact restrictions and lockdowns have been implemented due to the COVID-19 pandemic, leading to the transfer of most economical and educational activities into the virtual realm.

In Germany, innovations in the digital sector are quite complicated to implement due to the limitations of federalism. The government has few competencies in regard of education, since this is a federal issue. Financing is a matter of the communities, which often lack the budget for higher investments. An initiative to foster digitization in schools is the so-called digital pact, enabling the government to provide 5 billion Euros for the digitization of general education schools. Because of the COVID-19 pandemic the funds were raised, yet only hesitatingly used: After two years, only a third of the provided budget has been allocated (Kuhn, 2021).

A recent study (Mußmann et al., 2021) found out about a fundamental split between Germany’s schools: „While digital avantgarde schools use a digital strategy and a powerful infrastructure, teachers who work at late adopter schools miss practically everything needed for digital learning, from internet access to appropriate technology to support by the school management. Also further education for digital learning and teaching is offered far less often at late adopter schools.” (ibid.) Early adopter schools show high competencies in digital education and the relevant technological infrastructure, leading as an example for a future-proof digitized basic education.

### Self-check questions

* 1. Why is digitization in Germany particularly hard to implement?

(Technological issues, federalism, internet shutdowns)

## Inclusion and Diversity in Computer Science

Questions of inclusion and diversity are increasingly moving society. Since information technology also shapes society and its infrastructure, it must actively address these issues. Because of the importance of information technology, it is important that it address all of society, regardless of categories such as

* gender,
* ethnicity,
* worldview/religion,
* age/generation,
* disability, and
* sexual identity/sexual orientation.

In addition, a study by management consultants McKinsey suggests that companies with a diverse workforce are also more successful economically (Dixon-Fyle et al., 2020). Despite the call for more diversity, women are recently underrepresented in the field. However, the early days of computing are also marked by important pioneering women. The first programmable calculating machine, designed to read instructions for different programs, was conceived by Charles Babbage in Britain in 1833. Although it never worked, programs were already being developed for it, not least by Ada Lovelace (1815-1852), who thus went down in history as the first female programmer (Franzetti, 2019, p. 4). Actress Hedy Lamarr (1914-2000) is revered today as a computer pioneer because, among other things, she holds a patent for technology used in wireless connections such as Bluetooth and Wi-Fi. Throughout her life, however, she received little recognition for it (Dean et al., 2018).

In the 1960s, the United States launched the Apollo program with the goal of getting a man to the moon and back. This led to significant advances in many disciplines, not the least of which was computer science. Responsible for the program to develop the software aboard the lunar rockets was Margaret Hamilton (1902-1985). The development of the software is considered a considerable achievement and one of the reasons why the mission succeeded (Krichmayr, 2019). The role of Black women who worked as mathematicians and programmers on the Apollo project is recounted in the film Hidden Figures (Melfi et al., 2017).

It is all the more surprising that after this early phase, computer science has increasingly been perceived as a male discipline. Women continue to be significantly outnumbered in technical programs, often grouped under the acronym STEM (mathematics, computer science, natural sciences, and technology). In 2018, 17 percent of female students in the EU studied STEM subjects, but 42 percent of undergraduates (European Institute for Gender Equality, 2020). Accordingly, according to a study by the industry association Bitkom in Germany, “only one in seven applicants (15 percent) for a position for IT specialists (...) is female.” At the same time, the quota of women in first-year computer science studies fell to 28.9 percent in 2017 (Bitkom e.V., 2019). In the U.S., the figures are comparable. One reason for this, in addition to socially entrenched gender stereotypes, could be the lack of support for girls in technical subjects at schools.

In other categories of diversity, too, particularly with regard to the origin of employees, progress has been slow at best. Search engine operator Google is explicit in its commitment to diversity (“We are unequivocal in our belief that diversity and inclusion are critical to our success as a company”), yet 69 percent of its employees are male and only 2 percent are African-American. This appears to be due to more than just a lack of suitable candidates: In the Washington, DC, area, by comparison, 17.3 percent of employees in information and communications technology (ICT) jobs are African American (Wong, 2017).

One practical reason why diversity in computing is so important is the issue of bias in algorithms. The central role that ICT plays in the information society will become even more significant in the future, when artificial intelligence will increasingly make decisions that were previously made by humans - for example, about granting credit or pre-selecting candidates who have applied for a job. This makes it all the more important that such algorithms not only mimic the decision-making processes of white male Americans, but also make decisions as neutrally as possible. To ensure this, developers should, on the one hand, make transparent how the algorithms work. On the other hand, they should themselves work in diverse teams to minimize the bias of the algorithms (Bryson et al., 2020; O’Neil, 2017).

Unfortunately, women have been traditionally marginalized in all branches of natural sciences. Hence, the tech world, which is mostly fueled by mathematics, physics, and logic, continues to be a male dominated field of business. Until today, women fight for equality, participation and recognition, while many of the opposing forces are deeply embedded into the infrastructure of society. A well-known example for objective inequality is the controversial gender pay-gap. Another strongly debated method that aims to counter the effects of the marginilization of women in the business world in general is the women rate. In this model, the number of women in particular job branches is regulated by this rate. Problematic with such a rate is the ignorance of the basic qualification issue; only if society is able to overcome conservative gender-specific role models and spark enthusiasm for natural sciences in a growing number of elementary school girls, the participation of women and the number of qualified female competitors will substantially grow.

Despite a woman (Ada Lovelace) being the World’s first programmer, the number of women in the field of computer science is contemporarily not remotely on par with the amount of male computer scientists. This is mainly due to traditional gender-related notions of what women are supposed to choose as their working field. However, in an attempt to change this long-term situation, there is a great deal of initiatives that focus on sparking interest towards STEM disciplines among young women. STEM disciplines have traditionally been a male-dominated sphere, but this is slowly changing now that societal perspectives and expectations regarding gender roles are challenged, altered and ultimately transformed.

While the Bureau of Labor Statistics (BLS) projects computer science research jobs will grow 19 % by 2026, women earn only 18 % of all computer science bachelor’s degrees in the United States. (www.computerscience.org) Surprisingly, this situation has been substantially different, and in favor of the women. When computer technology first emerged during World War II and continuing into the 1960s, women made up most of the computing workforce. By 1970, however, women only accounted for 13,6 % of bachelor’s in computer science graduates. (ibid.) By 1984 the women’s share climbed up to 37 %, only to decline again to the current 18 %. If this illustrates anything, then it’s the fact that change comes in cycles – and rarely establishes lasting alterations.

### Self-check questions

1. Which categories of diversity play a role in information technology?

Gender, origin, world view/religion, age/generation, disability, sexual identity/sexual orientation.

2. Why is diversity important in information technology?

Bias in algorithms is prevented, companies with diverse workforces are more successful.

## Summary

The social impact of the information society is only beginning to emerge in many areas, but we can already see how significant it will be - whether this concerns the influence of social networks on political debate or the emotional health of their users, or the abruptly increased possibilities for monitoring people digitally. Desirable projects in education, for example, show how difficult successful implementation can be in the context of politics, social factors, and limited resources. To create systems that can make fair decisions, computer science should strive for much greater diversity. In this way, it can successfully contribute to major societal challenges such as the transformation to a sustainable society.

# Unit 5 – Infrastructure Vulnerability

**Study Goals**

On completion of this unit, you will be able to …

... identify social and technical infrastructures that are worth protecting.

... name and describe the major types of attacks and accidents that threaten critical infrastructure.

... recommend basic steps for IT risk management.

... name factors that are necessary for the implementation of IT security measures.

# 5. Infrastructure Vulnerability

## Introduction

Our modern data-driven information society is highly interconnected and intertwined. From this systemic complexity stems a high degree of inherent infrastructure vulnerability. Computer bugs, viruses or cyber attacks could all result in catastrophic fallout scenarios in the context of the Internet of Things and the vital supply chains managed by IoT. What would happen if the Internet went down for a day? The consequences would affect a large part of the population - in the USA, 20% of people use the Internet “almost constantly” and 73% at least daily (Nuwer, 2017). There are different views about the consequences for the economy - for stressed managers it could mean a quiet day, whereas self-employed people (for example, craftsmen) might be cut off from their customers and not get any orders. For larger companies, the consequences are difficult to assess. Although it is sometimes claimed that the loss of the Internet would lead to losses in the billions, an analysis of previous failures does not support this (Nuwer, 2017). Experts assume that an outage would not last too long because network operators and hardware manufacturers have made provisions for such cases. However, the example shows how much society depends on functioning technical infrastructures, and especially on information and communications technology (ICT). Which infrastructures are particularly worth protecting? What types of attacks can we prepare for, and how does this happen in practice? And last but not least: How vulnerable are our political and social infrastructures?

On the other hand, natural causes for fallouts of the power grid, like small animals electrocute themselves on the tracks, cannot be avoided and are in fact a greater threat to the integrity of the electric grid than attacks from hostile hackers. (Rawnsley, 2014) However, this situation might change with the development of cyber warfare.

Similarly, **internet fallouts** are deemed to be comparably hazardous. Supply chains would collapse, causing chaos and multiple states of emergency. While such scenarios are already well-studied and understood, they are far from outruled.

**Internet Fallouts**

The possibility of an internet fallout is still a given; however, much more often, internet shutdowns are deliberately implemented to suppress political protests or conflicting information.

However, more future-related scenarios must be regarded, too.

## 5.1 Attacks and accidents

The types of attacks on ICT infrastructure, and the motivations for them, are varied - from bored teenagers looking to test their skills to complex state-orchestrated attacks on other states and their infrastructure.

### Hackers

Hackers are individuals who penetrate other people’s IT systems without permission. This can be done for financial gain or for personal or political motives (Franzetti, 2019, p. 159). The motives for this range from the desire for attention or recognition by like-minded people to personal enrichment. Security researchers can also act as hackers, for example to test the security of IT infrastructures and report vulnerabilities to the operators. These so-called “white hat hackers” are distinguished from “black hat hackers” with dishonest intentions (Franzetti, 2019, p. 179). In contrast, as we will see, many states have built up enormous expertise in hacking, which they use to try to achieve their economic and military goals.

### Viruses

In the world of computing, viruses are malicious programs that, like biological viruses, spread independently and cause damage to affected computers. For example, the local address book can be read, whereupon the virus sends e-mails to all contacts, by means of which they can in turn become infected. Other viruses steal computer power or damage critical infrastructure (Franzetti, 2019, pp. 180-181).

### Ransomware

Software for hacker attacks is freely available, so that, for example, phishing attacks can be carried out with little technical understanding, in which users are tricked into sharing personal information such as logins and passwords. Recently, there has been an increase in so-called ransomware attacks, in which data or computer systems of individuals or organizations are encrypted and only released after payment of a ransom (Greengard, 2021).

### Accidents

In addition to malicious attacks, human errors are the primary contributors to infrastructure vulnerability. Organizations must therefore manage the risk of such errors and take steps to minimize it.

### Human Error

Human error often plays a critical role in the strategy of attackers. Phishing emails can trick employees into entering their passwords on fake websites that are actually operated by the attackers. In addition, every IT user has probably made mistakes themselves that have led to data loss - be it through missing backups, the accidental deletion of important files, or the loss or damage of important hardware.

### Bugs

Human errors also include security gaps due to programming errors, which experience has shown to be present in all complex software. These are referred to in English as bugs (“bugs”). In 2021, a case caused a stir in the trade press: Log4j, a widely used logging library in Apache Logging Services, had a vulnerability that allowed attackers to “execute their own program code on the target system and thus compromise the server” (BSI, 2022a). Due to the wide distribution of the library, log4j is considered one of the most serious IT security vulnerabilities in history - administrators worldwide had to update their installations to close it, which experts estimated would take “weeks, if not months” (Melanson, 2021, own translation).

Many large companies and other organizations operate so-called bug bounty programs, where the general public is invited to find and report such bugs, whereupon they receive a bonus (eng. bounty) if successful. This can be quite lucrative: In Microsoft’s Hyper-V Bounty Program, for example, bonuses of up to 250,000 US dollars are possible. Participating in such programs is a good way for budding white hat hackers to learn and increase the security of IT infrastructures at the same time. Unfortunately, this is not appreciated in all cases: it has happened several times that people who reported such breaches received criminal charges from affected parties instead of a bonus (Gießler, 2021). At the same time, such bonuses show how valuable critical security gaps are. Accordingly, a market for them has formed. Unknown vulnerabilities that have not been attacked or fixed so far are called “zero days” (because the manufacturing company had zero days to fix them). There are marketplaces for these as well - for example, zero days in Apple’s iOS operating system are sold for up to $2.5 million (LIFARS, 2021).

**Vulnerabilities**

systemic weak points that can become precarious through natural causes, accidents or attacks by hostile parties

### Disruptions to the Physical Infrastructure

**Vulnerabilities** of the ICT infrastructure also result from disruptions to the physical infrastructure. This begins with interruptions to the power or Internet supply and continues to include theft, fires or damage caused by floods and thunderstorms. An important unit of measurement for the operation of ICT infrastructures is uptime, i.e. the percentage of time that the system is operational. This is specified as a percentage (e.g., per year) and is an important component in contracts with cloud computing providers or data center operators. It should be noted that, for example, a guaranteed availability of 99.99% may still include a downtime of over 52 minutes per year during which the system is inoperable.

A rare, but potentially extremely high danger are solar flares or solar storms. In these, the Earth’s magnetic field is disturbed by protons and electrons emitted from the Sun in an unusually powerful eruption, which can cause massive damage to electricity grids worldwide. The last time this happened was in 1859; in 2012 there was a “near miss,” a solar flare that narrowly missed the Earth. Experts estimate the potential damage of such an event at up to 2 trillion US dollars (Phillips, 2014).

Another existential risk is posed by future, ultra-intelligent AI systems. In particular, scenarios in which AI becomes significantly more intelligent and more capable than humans pose distinct dangers and even threaten a major global catastrophe if the AI control problem isn’t solved entirely and reliably. Specifically, we focus on scenarios involving the following steps:

1) Humans create a seed AI that is able to undergo recursive self-improvement in either hardware or software.

2) The seed AI undergoes recursive self-improvement, resulting in a takeoff of successively more intelligent AIs.

3) The takeoff results in one or more superintelligent AI systems (ASIs).

4) The ASI(s) gain decisive strategic advantage over humanity, meaning “a level of technological and other advantages sufficient to enable it [the AI] to achieve complete world domination” (Bostrom, 2014; Yampolskiy 2015).

5) The ASI(s) uses their decisive strategic advantage to cause a major global catastrophe, such as (but not necessarily limited to) human extinction.

ASI is not deterred from acting unsafely. To deter is to persuade another agent to refrain from taking some action by convincing the agent that the action is not in their own interest. (Lierfeld, 2019) Even if an ASI has obtained a decisive strategic advantage and developed unsafe goals, it potentially could still be deterred from using its advantage to cause a catastrophe. However, Bostrom argues that an ASI with decisive strategic advantage would be undeterrable. (Bostrom, 2014)

On paper, the solution looks pretty easy: avoid that an AI would achieve a decisive strategic advantage. In reality, this is much more complicated as it appears at first sight, and only partly due to the many possible reasons sketched out in this subchapter.

### Self-check questions

1. Please please tick the correct statements.

* Hackers are in any case criminals. (W)
* Companies pay high premiums for discovering new security vulnerabilities. (R)

## 5.2 Technical Infrastructure

The question about which infrastructures are worth protecting quickly leads to a variety of answers. In public usage, the term “critical infrastructure” has become established. They are defined as “organizations and facilities with important significance for the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences.” (BMI, 2009). Specifically, Lechner et al. (2018) list the following critical infrastructures:

|  |  |
| --- | --- |
| Critical infrastructure (Lechner et al., 2018) | |
| Sector | Branche |
| Energy | Electricity |
| Gas |
| Mineral Oil |
| Information technology and telecommunikation | Telecommunication |
| Information technology |
| Transportation | Aviation |
| Maritime |
| Inland waterways |
| Rail transport |
| Road traffic |
| Logistics |
| Health | Medical care |
| Drugs and vaccines |
| Laboratories |
| Water | Public water supply |
| Sewage disposal |
| Nutrition | Food industry |
| Food Trade |
| Finance and insurance | Banks |
| Stock exchanges |
| Insurances |
| Financial services provider |
| State and administration | Government and administration |
| Parliament |
| Justice Facilities |
| Emergency / rescue services including civil protection |
| Media and culture | Radio (television and radio), printed and electronic press |
| Cultural asset |
| Symbolic buildings |

A large proportion of these infrastructures are also technical infrastructures (e.g., energy, information technology and telecommunications). Looking at the list, it also becomes clear that a large proportion of critical infrastructures depend to a greater or lesser extent on ICT (e.g., also state and administration, media and culture). This is illustrated below with a few examples.

### Internet

As one of the most important telecommunication networks, the Internet is a central critical infrastructure. Due to its history, it has a high level of robustness: Its precursor, the ARPANET, was created during the Cold War, in the 1960s, at a military research facility. The concept of a distributed computing network was seen as a possible protection against nuclear weapons attack. The decentralized, distributed nature of the Internet protects it from possible attacks. Nevertheless, attacks on central infrastructure are conceivable, such as undersea cables or major data centers.

The data centers maintained by large Internet companies such as Google or Amazon or by network operators are a central element of the Internet’s infrastructure. At the same time, they represent an important success factor, so they are often surrounded by an aura of mystery. In the example of the Google search engine, there was long speculation about the number and structure of the data centers, as it was assumed that they were particularly efficient and thus contributed significantly to the success of the search engine - if a search took too long, users might switch to another search engine. In the meantime, Google communicates more details about the data centers (Levy, 2012). Part of the security concept is redundancy - the system is designed to compensate for the failure of individual servers or an entire data center at any time (Google, 2022).

### Self-check questions:

1. Name 3 critical infrastructures (internet, stock market, power grid)

## 5.3 Political and Social Infrastructures

In addition to purely technical infrastructure, political and social infrastructures such as the state and administration or media and culture are infrastructures that are particularly worthy of protection. The dangers they face will be briefly discussed here.

### State IT security

The security and integrity of the ICT infrastructure also plays a crucial role for political and social infrastructures. In 2015, for example, Russian hackers attacked the IT system of the German Bundestag and stole more than 16 gigabytes of data - including numerous e-mails from members of parliament (Flade & Mascolo, 2020), which significantly impaired the work of the parliament and led to the temporary shutdown of the Bundestag’s entire network. Espionage by friendly countries is also a problem: In 2013, revelations by whistleblower Edward Snowden showed how the U.S. foreign intelligence agency NSA spied on millions of Internet users and also eavesdropped on politicians in friendly countries, such as German Chancellor Angela Merkel (Teichmann, 2018). Attacks by other states, however, are not the only risk to which state IT is exposed: In other cases, a single individual may be responsible. In 2018, a teenage hacker from Hessia obtained private data of members of the Bundestag, among others, which he made public on social media (Makartsev, 2020) - apparently without pursuing financial or political interests.

### Propaganda and Misinformation

The spread of propaganda and misinformation on the Internet poses a growing threat to politics and society. Misinformation or fake news are defined as “deliberately scattered messages on the WWW that do not correspond to the truth. They are intended to influence opinions, are often politically motivated, serve personal interest, or have a criminal intent” (Franzetti, 2019, p. 55). Propaganda is the term used to describe attempts to shape political opinion and influence people’s behavior accordingly. The social network Facebook prioritizes posts in the newsfeed that users get to see, the ones that generate a lot of comments and responses. In 2021, the “Facebook Files” showed, among other things, that Facebook has been at best half-hearted in addressing misinformation, even when it fuels aggression toward minorities (Hurtz et al., 2021). Thus, heightened hatred can lead to aggression and violence, and political misinformation is shared unchecked. The consequences were evident, for example, in the storming of the Capitol in Washington on January 6, 2021, which was fueled in part by misinformation on social media (Cellan-Jones, 2021).

Combating misinformation is the responsibility of the companies that operate the social networks. In addition, the European External Action Service (EEAS) has been specifically documenting disinformation campaigns emanating from the Russian Federation since 2015 to raise awareness and help its own citizens better recognize misinformation (euvsdisinfo.eu, 2022). The project has collected over 12,000 cases of disinformation in 15 different languages in its own database. A weekly newsletter provides information on ongoing developments.

### Self-check questions

1. How can states attack political and social infrastructures of other states?

Attacks on state ICT infrastructures, propaganda and misinformation to divide society.

## Summary

Economic, social and political infrastructures, and especially ICT infrastructures, play a vital role in our lives, but at the same time they are exposed to growing threats. These range from human error and threats from individuals to coordinated, technically sophisticated attacks by state actors. In addition, natural disasters also pose a threat. Risks are always a part of life, but it is advisable to manage them judiciously. Individuals and organizations should each analyze the risks they face and take appropriate countermeasures. Even very simple measures (for example, regular updates and backups) can effectively reduce threats. Organizations should give central priority to the management of IT security. Measures must be supported by both top management and employees to be effective.

# Unit 6 – Computer Science and the Military

**Study Goals**

Upon completion of this unit, you will be able to…

… identify and describe the connections between computer science and the military

… understand how the military influence upon civilian life is rooted in technological developments

… reflect on the ambivalence of technology

# 6. Computer Science and the Military

## Introduction

The world is in the midst of a digital arms race over robotics and autonomous weapons systems. Self-guided submarines, missiles, drones and vehicles are already in use. This technological power struggle, fought mainly between China and the U.S., is far more dangerous than the computer-based space race America won against Russia with the first moon landing. The digital arms race is about much more than mere technological prestige. It threatens a global political monopoly. In this battle for technological world domination, unnoticed by many, the winner could succeed in imposing its economic and sociopolitical value system on the losers. In the future, fully autonomous weapon systems could select targets and carry out attacks without any relevant human influence. Robots would then make the decision about life and death of humans. From a rational efficiency perspective, unmanned drones may already identify targets more clearly and select more adequate means to eliminate them. However, if the target is not a chemical weapons factory but a human being, the ethical question arises as to whether the algorithm-controlled death of the latter is at all justifiable and under what conditions.

## 6.1 Military as the Driver of Computer Science

The military-industrial complex shares decades of successful cooperation, ultimately culminating in robotic breakthroughs like Boston Dynamics’ Big Dog or the humanoid Atlas.

The human tendency to wage war contradicts the rational world view and the pacifist basic attitude of many computer scientists. Nevertheless, they cannot avoid dealing with global political issues. The physicist Albert Einstein was concerned with the question of why mankind wages war at the outbreak of the Second World War at the latest. In his correspondence with Sigmund Freud, the founder of psychoanalysis, he argued in favor of a supranational organization “which should settle all conflicts between states peacefully” (RBB, 2005): “The goal of securing international peace has been recognized in its importance by the truly significant people of earlier generations. The development of technology in our time, however, makes this ethical postulate a question of existence for today’s civilized mankind, and active participation in the solution of the problem of peace a matter of conscience which no man conscious of moral responsibility can avoid.” (Seelig & Einstein, 2017, p. 53). Freud responded skeptically: the destructive instinct is innate in human beings, so “there is no prospect of trying to abolish man’s aggressive tendencies” (Freud, 1994, p. 173). Thus, in practice, wars continue to take place, and modern states continue to maintain armed forces, if only to protect themselves from the threat of other states.

The emergence of computer science and information and communications technology (ICT) was largely driven by wars and other conflicts. Wars have long taken place in virtual space, and technology has also changed conventional warfare. The military represents an important industry and is a major employer of computer scientists. Even those who do not work directly for the military may be unintentionally supporting it if the civilian technology he or she is working on is used by the military.

The Cold War (1947-1989) between NATO and the Warsaw Pact has been labeled “cold” because there was no direct combat between the main adversaries - the United States and the Soviet Union. The concept of mutually assured destruction, which prevented either side from attacking, is associated with another great computer pioneer, John von Neumann, who defined the fundamentals of hardware architecture and made significant contributions to several other fields, from economics to quantum mechanics (Veisdal, 2021). This period also saw the emergence of ARPANET, the precursor to the Internet. The concept of a distributed computing network that could not be destroyed in one single swoop fits well with the era when a nuclear attack was considered an actual threat.

Recent advances in computer technology can also be traced back to a large extent to military projects. Here, developments in the field of artificial intelligence (AI) are particularly noteworthy (Miebach, 2020, pp. 189-193). Driven by Turing, systems were developed after the war to mimic human capabilities. In the 1980s, it turned out that the hopes were in many cases exaggerated, and quite a few projects were discontinued (“AI winter”). Since about 2010, there have been new successes in connection with so-called Deep Learning systems, which use more mathematically sophisticated methods and had much larger amounts of data available for machine learning. This led to significant progress, for example in image recognition or machine translation. The driver here was no longer primarily the military, but Internet companies such as Google, Facebook and Amazon (Miebach, 2020, p. 192).

Even as a pacifist, one must admit that war and international conflict have tremendously accelerated the development of computer science. The attitude of war as the “father of all things” has existed since antiquity (Heraclitus), but it has also often been used as a justification for unethical actions: “You know what the fellow said - in Italy, for thirty years under the Borgias, they had warfare, terror, murder and bloodshed, but they produced Michelangelo, Leonardo da Vinci and the Renaissance. In Switzerland, they had brotherly love, they had five hundred years of democracy and peace - and what did that produce? The cuckoo clock” (Reed et al., 1950). In this case, Harry Lime (played by Orson Welles), the antagonist in the film “The Third Man”, makes profits by trading in adulterated drugs, but also accepts the suffering of those treated with them.

### Self-check questions

1. Why was the internet designed as a distributed entwork?

To make it resistent against nuclear attacks on some of its knots.

## Cyber War

During the advent of digitization and the data-driven society, a new kind of warfare evolved. This warfare was aiming at digital battlefields, but the casualties resulted in harm in the real world. Cyber attacks often aim at neuralgic points of the infrastructure, as in the hacking of a German hospital in Düsseldorf back in 2020 by alleged Russian cyber terrorists. (Karabasz, 2022) While methods of cyber warfare can be mere data theft, like in regular hacking, it is the intention of methodical espionage for military, political or terrorist goals that sets the category of cyber war apart from hacking. It is notable that the three categories of aims – military, political, terrorism – may share more mutual ground than expected at first sight. In fact, all three categories are intertwined in a mutual symbiotic relationship. The military depends on political decisions, while the political system depends on a reliable and well-organized military apparatus. On the other hand, terrorism is interfering with the political and defensive sectors in multiple ways, and lastly it is entirely a matter of perspective to call a violent attack an act of military intervention or an act of terrorism.

b

Darknet refers to a portion of the internet that is not indexed by search engines and can only be accessed through special software, allowing users to remain anonymous and often engaging in illicit activities such as illegal trade, hacking, and communication.

The blurring borders between the described categories make for a high degree of ambivalence and uncertainty in the field of cyber war. This is mostly due to the nature of cyber attacks: they are clandestine. Often these interventions are black ops in the literal sense, as they operate in the **Darknet**. This counterworld to the low-threshold internet enables for hiring all kinds of specialists and the acquisition of the most exotic bug code. The clandestine strategies of cyberwar tend to result in high uncertainty. In some cases the cyber attacks are only detected when the damage is already done, in others they are completely overseen for a long time. Akin infection transferring bacteria that cannot be seen by the unassisted human eye, intruding cyber warriors are invisible to a certain degree. In contrast to traditional military warfare, cyber warfare explicitly attacks civilian infrastructure. This distinction may mark cyber warfare as even more unethical. Another notable aspect of this method is that it takes place on digital battlefields, however results in possible catastrophes in the real world.

The interconnectedness of our technological realm and especially the advent of cyber-physical systems like the Industrial Internet of Things make for a great systemic vulnerability. As so many systems are interconnected and intertwined with one another, a hostile bug could contaminate the whole chain, potentially causing a multi-level fallout. The expectable results of a major fallout of the electric grid have been pondered by simulations and are particularly alerting in terms of the demographic of the anticipated casualties and other social implications. The most vulnerable parts of the population – babies, old people, chronically ill people – would die within the first week of a nation-wide fallout. All cooled food and medicine would be rotten, the supply chains would collapse and all trading would come to an abrupt halt. Ironically, homeless people would be among the less affected populations, as for them not much would change. Despite likely social unrest, that is.

Conservative political world leaders like Putin or Trump have long noticed the power of cyber armies of chat bots that are able to push elections into the desired direction and bend the will of the population. (Clegg, 2019) As of now, there are more fake bots than online profiles of existing people. (Rusche / Lierfeld, 2022) This tendency is not likely to shift back any time soon. And clearly, this is a systemic issue that largely supports the effectiveness of cyber warfare methods.

### Digital Offense and Defense

Not surprisingly, the digital world plays a central role in warfare. The term “cyber war” or cyber war refers to “on the one hand, the warlike confrontation in and around virtual space, cyberspace, using means primarily from the field of information technology” (Wikipedia, 2022b), and on the other hand, “the highly technical forms of war in the information age that are based on extensive computerization, electronization and networking of almost all military areas and concerns” (Wikipedia, 2022b). The possibilities for inflicting damage on an adversary in the event of war are also considerable in virtual space. Blum (2020) lists the following instruments of cyberwar:

**Blockchain**

This technology offers a decentralized data flow system that is secured by encryption. It enables for cryptocurrencies and coming metaverse use cases.

* Worms, viruses, and manipulated chips as direct-action weapons that can be used to gain access to an opponent’s IT systems
* Market platforms as weapons - here, personal data of the users of platforms such as Facebook are used to create profiles “with the aim of explaining, modeling and possibly even predicting behavior in the future” (U. Blum, 2020, p. 847).
* Metadata and cyberintelligence: “If in a normal war the domination of geographic spaces and in economic war the domination of product spaces is of importance, in cyberwar the domination of a time field in a data continuum is of interest. The idea is to reconstruct what has been, analogous to reconstructing the deployment of an enemy, with the goal of being able to estimate or predict future actions” (U. Blum, 2020, p. 847).
* Digital currencies and power sharing through **blockchain** technology: here, price fluctuations can be caused, for example, by hacker attacks.

**Denial of Service**

Cyber attack in which the attacker aims to block a website or a network to take it down. Regularly this happens through a huge number of requests.

* Darknet and cryptography: technologies that enable anonymous web browsing and secure communications.

Orr (2018) defines cyberwar as “using computer technology to sabotage the electronic or physical resources of a state or organization.” She lists examples of how this has already been accomplished-including viruses, malware, ransomware, and **denial of service** (DoS) attacks and presents some important cases. In keeping with the logic of war, this also forces peaceful nations to build capacity to defend against such attacks. The Bundeswehr defines five spaces or dimensions in which military operations can take place (Deutscher Bundestag, 2021):

1. Cyber and information space
2. Land
3. Air
4. Sea
5. Space

This shows the great importance attached to cyber warfare and how important it is for the Bundeswehr to be able to defend itself in this area. In order to recruit the necessary personnel and build up the corresponding expertise in the field of digitization, the Bundeswehr is building up a so-called cyber reserve with former soldiers, but also civilians, who will help to secure Bundeswehr IT systems in an emergency. Since new expertise is always needed for this purpose, the cyber reserve is broader than the general reserve of the Bundeswehr; it addresses not only former soldiers but also experts from industry (Bundeswehr, 2021).

### Digital Components in Weapons

Warfare itself has changed significantly due to digitalization, which in turn leads to new challenges. This has obvious advantages for the warring nation and its soldiers, but also raises ethical questions. This will be demonstrated here using the example of drones. Drones are unmanned aerial vehicles that can be used in the military for intelligence gathering. However, there are also armed drones that are used in combat operations. From the point of view of the warring nation, these have the advantage that they enable targeted strikes against individuals or small groups compared to conventional weapons. In addition, their own soldiers are not at risk, as the drones are controlled remotely (in the case of foreign missions, usually from the soldiers’ home country). One objection to drones is that - as with all attacks - there is a risk of killing uninvolved civilians. Anonymous killing from afar potentially violates Just War principles, including humanity, necessity, and proportionality. Threat warfare is also particularly stressful for the attackers. Last but not least, it is also unclear whether drone strikes are effective at all (Glazebrook, 2019)

### War of Words: Propaganda, Fake News

An important component of war has always been the war of words: the spread of propaganda and misinformation on the Internet plays a central role in today’s conflicts. Misinformation or fake news are defined as “deliberately scattered messages on the WWW that do not correspond to the truth. They are intended to influence opinions, are often politically motivated, serve personal interest, or have a criminal intent.” (Franzetti, 2019, p. 55) Propaganda as attempts to shape political opinion and influence people’s behavior accordingly is as powerful and effective as since its inception. Both are - like cyber war - important components of hybrid warfare, which is a hybrid form of military and non-military attacks intended to blur the threshold between war and peace (U. Blum, 2020).

The possibilities for spreading propaganda and false news have increased significantly due to digitalization and especially the proliferation of social media, and they are used by conflict parties as a matter of course. Misinformation disseminated on a large scale by automated accounts sows doubts among the population, and their viewpoints can be successfully manipulated. Examples of this can be demonstrated both in relation to the COVID-19 pandemic and its response and in relation to the war in Ukraine (Schreiber, 2022).

Conversely, due to their asymmetrical structure, social media also offer attacked parties the opportunity to reach the attention of the world public and to spread their view of things: “Because in 2022, information is power. And one of the many huge unexpected geopolitical shifts of the last week is that this power has been returned to the people” (Cadwalladr, 2022). One example is Volodymyr Selenskyj, the president of Ukraine, who successfully used social media such as TikTok, Instagram, and Twitter after the Russian attack on his country, not only boosting the morale of the population but also earning high respect abroad as “hybrid warfare’s first hybrid leader” (Cadwalladr, 2022).

Open Source Intelligence

This points to an aspect that, despite all the wars, gives some hope, namely that the individual may no longer be completely helpless in the face of war. The concept of Open Source Intelligence (OSINT) makes it possible for basically anyone with a smartphone to intervene in the war effort. For example, people who are not directly involved in combat operations (and who have an Internet connection) can track the movements of the enemy to support the defense: “Every tank is being logged. Every truck and every troop movement is tracked, registered and added to open source maps and databases. This is a country of 44 million people recording every twitch their Russian invaders make. It’s a firehose of real-time information that, with the help of this volunteer army, is being turned into real-time military strategy.” (Cadwalladr, 2022). The OSINT strategy has been pursued since at least the “Arab Spring” of the 2010s by volunteers who organize themselves and evaluate satellite imagery in their spare time, for example, to document troop movements (Reuter, 2022).

The digital arsenal also includes hacker attacks to paralyze supply networks (electricity, gas, water), telephone services, companies and government apparatuses. In this context, the award of German 5G exploitation rights to the globally active Chinese telecommunications giant Huawei is also problematic. Should the company be fundamentally excluded from the award procedure in order to rule out Chinese infiltration of the Western infrastructure, or is it only a question of appropriate control mechanisms and security standards to which Huawei would have to submit?

In the hands of totalitarian states, digital dominance could lead to the erosion of the Western community of values with its acquired rights to freedom. Digital election interference is already endangering citizens’ trust in the stability of democratically elected political institutions and undermining the legitimacy of free elections. Democracy itself is at stake, which is being attacked by totalitarian systems worldwide by means of digital warfare. Over 1000 high profile artificial intelligence experts and leading researchers have signed an open letter warning of a „military artificial arms race” and calling for a ban on „offensive autonomous weapons”. The letter, presented at the International Joint conference in Buones Aires, Argentina, was signed by Tesla’s Elon Musk, Apple Co-founder Steve Wozniak, DeepMind chief executive Demis Hassabis and professor Stephen Hawking along with 1000 leading AI and robotics researchers. (Lierfeld, 2019)

DARPA (as part of the military—industrial complex) is one of the biggest investors in the field of machine learning. From the 1960s through the 1990s, DARPA funded more AI research than private corporations and any other branch of the government. (Barrat, 2014) Thus, DARPA is widely regarded as the most decisive factor that made the computer revolution take place. A recent annual budget allocates $61,3 million to a category called Machine Learning, and $49,3 million to Cognitive Computing. (ibid.) This saved DARPA its status as biggest player in the game, until Elon Musk’s AI initiative OpenAI has started off with a massive budget of one billion dollars in December 2015.

### Self-Check Questions

1. Please tick the correct answers.

* Drones are effective and ethical as weapons. (W)
* The Bundeswehr prepares for attacks from space. (R)
* Social media can be used for both offense and defense in the event of war. (R)

1. How does the Bundeswehr intend to build up the necessary expertise in cyber security?

Establishment of a “cyber reserve” with knowledgeable civilians

## Dual Use

Technology is often ambivalent in the sense that it can be utilized for mankind’s mutual benefit or for destructive goals like warfare. Dual-use technologies are those used for both civilian and military fields of application. The double purpose constituted by dual use technology is relevant only for a fraction of technology; however, these ambivalent tools or materials are potentially much more dangerous than common goods. Hence, dual use technology is usually subject to approval. Their import and export is restricted and thoroughly tracked and recorded.

Technologies developed for military purposes can often also be used in the civilian sector (and vice versa). This is described by the term dual use or dual-use capability. This includes technologies such as nuclear power (energy generation vs. atomic bomb), rockets (space flight vs. offensive weapon) and, of course, the majority of innovations in the field of ITC, even technologies where one would not initially expect it. Sony’s PlayStation 2 game console, for example, was considered a dual use technology because of its advanced computing power. The case of the Hololens 2, a pair of mixed reality glasses for home use that Microsoft unveiled in 2019, caused some discussion. When it emerged that the company had simultaneously signed a contract with the U.S. Army to use the Hololens 2 for training purposes and battlefield support, massive protests from employees ensued-after all, Microsoft committed to ethical principles in deals with the military (Riley & Burke, 2019).

New moral challenges arise from the fact that many products can be used in military contexts: Companies developing new technologies (and their employees) must ultimately always think through the purposes for which they could be used and what the consequences would be. We have seen that advances in technologies such as artificial intelligence are now driven by private companies such as Google, Amazon, and Facebook, rather than by the military as in the 1960s. Thus, new technologies will always arouse the military’s desires, and manufacturers must consider whether and under what conditions they are willing to cooperate. Ultimately, it is advisable to agree on writing on basic guidelines, such as purposes for which the technology will not be used.

In this context, the case of the search engine Google is particularly interesting, as it had a high moral standard from the very beginning (“Don’t be evil”). This claim is taken very seriously by many employees: In 2018, they enforced that Google withdrew from a project that wanted to use artificial intelligence software to analyze images collected by military drones. The developers were concerned that their technology could ultimately be used to kill people. Nonetheless, parts of the company still want to work with the military, so discussions continue. While the company has ruled out making its AI technology available for weapons, its parent company Alphabet still invests in related startups (Brewster, 2020).

### Dual Use Example: Drones

Drone technology is surely a vivid example for such an inherently ambivalent technology. Military drones are now semi-autonomous and are thus on the verge of making their own ethically relevant decisions. This is a major problem that could be solved by the use of brain-computer interfaces (BCIs); drones could be controlled by interconnected human pilots who would be responsible for the decision to attack. Such a solution must be found, as it is fundamentally unethical to allow machines to make decisions about life or death of human beings. Therefore, it is imperative that a human decision-maker remains in the chain of command, at least now and for the foreseeable future. We should not “expect technological development to ‘naturally’ lead to responsibly deployable AI in defense. Even the development of irresponsible AI-based weapons technology is possible and may be sought by adversaries.” (Koch, 2020)

Dubai-based drone and space aviation enterprise CYNAX (www.cynax.com) builds drones that operate both in the civilian and the military field; but their devices are detector drones that scan the ground to the depth of 100 meters below. Due to six different sensory systems, Cynax drones are able to identify whatever materials they find in the ground. Originally designed to detect mines, the scope of civilian applications quickly broadened.

But does the current technology, may it be weapons of math destructions or war drones, obey to the famous three laws of robotics, as demanded by scientist and science fiction writer Isaac Asimov back in the 1960s? To approach this question, we must first decide whether or not drones are robots. A drone is essentially an Unmanned Aerial Vehicle (UAV). But most drones are multi-purpose mechatronic devices, some of which are partly controlled by artificial intelligence. Hence, the more advanced multi-purpose variants of drones should surely count as robots.

The three robotic laws by Asimov (1942) are:

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey orders given by human beings except where such orders would conflict with the First Law.
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

While Asimov surely achieved to create compact laws with a coherent logic supporting them, his robot laws are deemed to fail due to our ambivalent and context-dependent language. There is simply too much room left for interpretation. For instance, the “intended harm” seems to refer to physical rather than psychological harm. Furthermore, the term is only well-defined in legislative contexts. In the near future, drone pilots are going to carry out orchestrated attacks through thought alone, making use of brain-computer interface technology. Taking Asimov’s laws literally, any drone that attacks or kills human beings has to be regarded as violating the first law. Does this mean Asimov’s laws failed regarding the reality of semi-autonomous drones? Doesn’t it apply for cases in which human beings are still in the decision chain? Or does it mean we have to bring these laws to strict application?

Koch warns to take ethical research serious regarding the challenges at hand: „Ethical considerations in the research and development of AI in defense should therefore be actively encouraged and its responsible use technically facilitated. This includes designing well-thought-out rules of engagement (RoE) that must consider the risks of AI in defense and permeate technical system design.” (Koch, 2020)

The concept of personal responsibility and accountability could be profoundly altered by the use of intelligent technologies; in fact, these formerly purely human characteristics could be extended to the realm of machine intelligence or even transferred entirely from humans to AI. “Conclusions from ongoing research lead us to the notions of technical controllability and personal responsibility, which appear as technical design principles for the use of AI in defense. […] A discussion of the challenges and research questions that need to be answered to enable its technical implementation seems to indicate that AI in defense may lead to a paradigm shift in systems engineering.” (ibid.)

### Self-check questions

What technology can be used for military purposes as well?

* Nuclear power (R)
* Rockets (R)
* Machine guns (R)
* Gaming consoles (R)

## Summary

The peaceful world in which all conflicts are settled is something not only Albert Einstein wished for, but also many computer scientists. Computer science owes much of its progress to military uses, and of course digital technology plays a central role in today’s conflicts - both in attack and defense. Social media and disinformation also play a critical role in hybrid warfare. The military is a major employer in the ICT industry worldwide, but it is up to the conscience of each computer scientist to decide what kind of systems they work on. As the example of dual use shows, it is not always easy to separate civilian and military use, so companies should set themselves appropriate ethical guidelines.

# Unit 7 – Responsibility in Computer Science

**Study Goals**

Upon completion of this unit, you will be able to…

... explain the importance of ethical aspects in computer science.

... name important ethical principles.

... name the role of ethics in algorithmic decision-making.

... recommend mechanisms for implementing responsibility in organizations.

# 7. Responsibility in Computer Science

## Introduction

Questions about the social implications of computer science and the information and communication technology (ICT) it develops inevitably lead to questions about responsibility and about the right, ethical way to act and do business. Due to technological progress - not only in the field of informatics - ethical questions have gained a broader relevance, especially since the 20th century. Inventions such as the internet or the atomic bomb increasingly affect all of humanity, no longer – as in earlier times – only a small part of it. As examples of ethical issues, consider:

* Systems based on artificial intelligence will potentially put 47% of jobs in the US at risk (Frey & Osborne, 2013). Who would be responsible if this happens? And should they be developed anyway?
* American Internet corporations such as Alphabet (Google) and Meta (Facebook) are increasingly taking monopoly-like positions in various markets. Is that acceptable? What happens when their systems promote the division of democratic societies and violence against ethnic minorities?
* The military is a major employer of computer scientists. Is it ethical to work for a company that may be marketing weapons for wars of aggression? What about working for a company whose products can be used in both civilian and military applications, such as Microsoft’s Hololens 2 mixed reality glasses (Riley & Burke, 2019)?

Helping to answer such questions can be ethics, which, as part of practical philosophy, has been concerned since antiquity with the evaluation of human actions and,in particular, with questions of morality. In the 4th century BC, the Greek philosopher Aristotle addressed the question of how to be a good person in the Nicomachean Ethics. He saw bliss, defined as the activity of the soul according to perfect virtue in a full human life, as the highest good and ultimate goal of all action. He advocated an ethic of moderation to restrain the irrational part of the soul and to find the right middle between excess and deficiency. His ideas, not only in the field of ethics, formed the basis for Western as well as Islamic science and philosophy until the 17th century (Hart-Davis, 2015, pp. 105, 131).

Ethics establishes criteria for good and bad actions, but its values are not universal; rather, they are historically and socially shaped. The question of how to operate and manage ethically is one that individuals, organizations, and societies must continually ask themselves. Classical systems of ethics help to answer such questions. But they have also been adapted over the centuries to address, for example, the ethical implications of modern technologies. So how can we use new technologies in ways that maximize their benefits and minimize their harms? There is no general answer, but there are promising approaches, guidelines, and mechanisms that we can draw on.

## Ethics of Responsibility According to Jonas

**Ethics**

A millenia-old discipline of philosophy that ponders the humanistic decision making. Closely attached to moral, ethics aims for practical solutions, especially regarding avoiding dilemma situations, in contrast to moral, which is more abstract.

The modern history of **ethics** is essentially shaped by the German philosopher Immanuel Kant (1724-1804), who defined the so-called Categorical Imperative as the principle of moral action in his “Critique of Practical Reason”: “Act only according to that maxim by which you can at the same time will that it should become a universal law.” This provides the individual with a simple ethical guideline: What would it look like if my decision or action served as the basis for a general law? Or rather: What if everyone acted that way?

Against the background of technological progress in the 20th century, the German-American philosopher Hans Jonas (1903-1993) developed Kant’s ideas further. Inspired by the early environmental movement in (West) Germany in the 1970s, he addresses questions such as human responsibility for the survival of ecosystems and the role of the individual(s) in doing so in “The Principle of Responsibility: Attempting an Ethics for Technological Civilization” (Jonas, 1979). Jonas shows that because of technological advances, the actions of individuals can affect all of humanity. Therefore, their responsibility no longer refers only to the immediate area (such as their immediate surroundings), but for the first time to all of humanity, including future generations. Thus, he argues for the radical ecological responsibility of individuals, organizations, and states, placing himself in direct opposition to the belief in technology of the time. Borrowing from Kant, the maxim he formulates is: “Act in such a way that the effects of your action are compatible with the permanence of genuine human life on earth” (Jonas, 1979, p. 36). In particular, he also points to the ethical significance of technology. As it shapes more and more areas of life, he argues, it must also submit to moral principles:

“If nothing succeeds like success, nothing captivates like success. Whatever else belongs to the fullness of man is outshone in prestige by the expansion of his power, and so this expansion, by binding more and more of man’s powers to its business, is accompanied by a shrinking of his concept of self and being. (...) If the sphere of making has penetrated the space of essential action, then morality must penetrate the sphere of making from which it formerly kept itself aloof, and it must do so in the form of public politics” (Jonas, 1979). In his later work, Jonas focussed onto rather anthropological perspectives, musing about the urgency and the conditions of a course of action that is suited to guarantee or at least maximize the chances of the persistance of human life as a species. Jonas aimed to overcome traditional dualist notions by referring at the core mental processes to the existence of a metabolism. An entity that possesses a metabolism possesses an elemental trait of life, as Jonas concluded. (Jonas, 1979) The mental, depending on the specific conditions of its metabolism, comes to life in various forms; their mutual condition is being alive because of metabolic activity. (ibid.) From this natural philosophical perspective, Jonas embarked to more general ethical reasonings which incluce mankind in the light of technology and the responsibility that stems from it.

Based on the ethics of discourse, the inviolable dignity of the human being encompasses not only all present, but also all future living beings, whose claims are to be represented by us as advocates. We are obliged to demand the rights to life and discourse of future generations of humanity by means of argumentation and to refrain from anything that could impair the “permanence of genuine human life on earth” (Jonas, 1979). The future of humanity is – at least hypothetically – at risk in the digital age and at the same time so valuable that we must take responsibility for the preservation of our future living conditions on this planet.

Freedom is also the central concept in Hans Jonas’ philosophy. In metabolism he recognizes the specific mode of being of the organic. Without metabolism there is no organism, no life. (Jonas, 1979) Through metabolism everything organic is connected with each other. (ibid.) The metabolism connects the inside of every living being with its outside world. (ibid.) By means of the criterion of freedom, which Hans Jonas is already able to recognize in metabolism itself, he clarifies an ontological gradation from the unicellular organism to the human being. (Rusche / Lierfeld, 2022) A maximum of freedom opens up to man morally ambivalent possibilities for evil and at the same time calls him to moral responsibility.

What is the responsibility that results from the reflection on human freedom? First and foremost, it consists in affirming life. (ibid.) This will to live is also already inherent in metabolism. However, only man, thanks to his freedom and his intelligence-based capacity for reflection, is capable of creating the conditions for life worthy of man. Because he is able to do this, he also bears responsibility for the future possibility of a life worthy of human beings on our planet. Only the human being, no other living being and no robot is able to take over this responsibility. Some dolphins may save human lives, but their radius of action is limited to individual cases. Robots, equipped with advanced artificial intelligence, can support humans with appropriate programming to make the world a habitable place for all living beings in the future. However, AI needs humans and their programming commands to do so.

Life is bound to the process of evolution. The human being reflecting his progressive physical decay becomes aware of his finiteness and wants to overcome it. Silicon-based artificial systems have no interest in survival. But they could enable man to live longer and longer through technological enhancement. Even overcoming death does not seem out of the question to the futurists.

Will humans in the future have the freedom to choose between life and death, between continued life through silicon-based transformation and biological-organic death? Would this freedom of choice be desirable, or would man thus deprive himself of the essence of his existence, because the finiteness of life is an important prerequisite for its meaningfulness? Organisms strive for life, the human being beyond that for sense. Would an immortal life be the best condition to develop all potentials and to become a real human being? Or meaningless, because with increasing age everything seems to the human being equivalent, boring and finally laborious? Is the end of life a protection against boredom and routine as well as a “chance to preserve the spontaneity of life”? (Jonas, 1979).

Cyborg:

Short for “cybernetic organism”: being that combines both biological and technological components. This can range from simple wearable technology to advanced prosthetics or implants that enhance human capabilities or replace lost function, creating a hybrid between human and machine.

Formulated from the value-ethical perspective of Hans Jonas, the future of humanity is something so valuable that we cannot deny it. The responsibility that stems from this is of historical weight, especially since mankind is standing at the crossroads of merging together with digital technology entirely. Thus we must face the high likeliness that humanity will inevitably continue to diversify, merging together with technology and establishing new forms of beings.

**Cyborgs**, as we already know them in different forms, are only a forecast upon the wide spectrum of novel beings. Some of them might be entirely digital. Are they still counting as life? At least they lack a metabolism. Do these future entities need an artificial metabolism to count as forms of life? What about artificial life? There are already robotic cells based upon biological stem cells that show all key trades of life, including a metabolism. It appears that we as a species will have to adapt and widen our concepts of „life” and „beings” in the near future.

### Self-check questions

1. Why was a reformulation of the categorical imperative necessary in the 20th century?

Through new technology, human actions potentially impact all of humanity and future generations.

2.Complete:

The central phrase in Jonah’s ethic of responsibility is: “Act in such a way that the effects of your action are compatible with the permanence of genuine human life on earth.”

## Ethical Guidelines for Computer Science in Society

Many computer scientists are aware of the responsibility for the consequences of their actions. The most important professional association in Germany, the Gesellschaft für Informatik e. V. (GI), which was founded in 1969, repeatedly takes a stand on social issues.

The GI first defined ethical guidelines for its members back in 1994 and committed itself and its members to adhering to these guidelines. After intensive debates, the current version was adopted in 2018 (GI, 2018). In the preamble, the authors formulate the wish “that professional ethical or moral conflicts become the subject of joint reflection and action. The guidelines are intended to provide guidance to GI members and, beyond that, to all people who design, produce, operate, or use IT systems” (GI, 2018). They also invoke the values of the Basic Law of the Federal Republic of Germany and the Charter of Fundamental Rights of the European Union. Among other things, the guidelines include an obligation for members to critically scrutinize their actions in social discourse (§ 4) – combined with a call for civil courage that also justifies public whistleblowing (§ 9). The guidelines do not deal with specific dangers or technologies – instead, the authors point out that “there can be no conclusive instructions or rigid rules for morally appropriate action. This makes sense insofar as technologies change and develop rapidly - moral principles, on the other hand, should remain stable over a longer period of time. Because of their importance, the guidelines are reproduced in full below:

### Art. 1 Professional Competence

The GI member appropriates, considers, and constructively critiques the state of the art in science and technology in his or her field of expertise. The GI member continuously improves his or her professional competence.

### Art. 2 Technical Competence and Communicative Competence

The GI member continuously improves his technical competence and communicative competence so that he understands the requirements for the design, production, operation and use of IT systems and their technical and factual interrelationships that affect his tasks. In order to be able to assess the effects of IT systems in the application environment and to propose suitable solutions, it is necessary to be prepared to understand and take into account the rights, needs and interests of those affected.

### Art. 3 Legal Competence

The GI member knows and observes the relevant legal regulations in the design, production, operation and use of IT systems. The GI member participates in the design of legal regulations within the scope of his/her technical and professional competence.

### Art. 4 Ability to Judge

The GI member develops his ability to judge in order to be able to participate in design processes in individual and collective responsibility. This requires the willingness to critically question and evaluate one’s own and collective actions in social discourse and to recognize the limits of one’s own ability to judge.

### Art. 5 Working Conditions

The GI member is committed to socially acceptable working conditions with opportunities for further training and development.

### Art. 6 Organizational Structures

The GI member actively advocates organizational structures that promote and enable socially acceptable working conditions and the assumption of individual and collective responsibility.

### Art. 7 Teaching and Learning

The GI member who teaches computer science promotes critical thinking skills, prepares learners for their individual and community responsibilities, and is a role model in doing so. The GI member who learns computer science in school, college, or continuing education requires this of those who teach.

### Art. 8 Research

The GI member who conducts research in the field of computer science observes the rules of good scientific practice in the research process. This includes in particular openness and transparency in dealing with criticism and conflicts of interest, the ability to express and accept criticism, and the willingness to address the implications of one’s own scientific work in the research process. Scientific research comes up against limits. These must be made understandable.

### Art. 9 Courage

The GI member courageously stands up for the protection and preservation of human dignity, even if laws, treaties or other norms do not explicitly demand this or even contradict it. This also applies in situations in which his or her duties to clients conflict with his or her responsibilities to others who are affected. In justified exceptional cases, this may also include public reporting of grievances.

### Art. 10 Social Responsibility

The GI member shall contribute to the improvement of local and global living conditions with the design, production, operation and use of IT systems. The GI member bears responsibility for the social and societal impact of its work. Through its influence on the positioning, marketing and further development of IT systems, it shall contribute to their socially acceptable and sustainable use.

### Art. 11 Enabling Self-Determination

The GI member shall work to enable those affected by IT systems to participate appropriately in the design of these systems and their conditions of use. This applies in particular to systems that can be used to influence, control and monitor the data subjects.

### Art. 12 The Society for Computer Science

The Gesellschaft für Informatik encourages its members to follow the guidelines in every situation. In cases of conflict, the GI attempts to mediate between the parties involved.

(GI, 2018)

### Self-check questions

1. What principles does the GI invoke in its ethical guidelines?

* Basic law (R)
* Civil code (W)
* Charter of Fundamental Rights of the EU (R)
* Categorical Imperative (W)

## Algorithmic decision making

Decision making by algorithms, also known as algorithmic decision making (ADM), is an issue of ever-raising relevance, since ADM is implemented within a rising number of contexts. The applications of ADM are widespread and versatile, as they range from mere job selection contexts to literal life-and-death scenarios within the health-care sector. Of particular importance is the fight on algorithmic bias, a phenomenon of biased machine decisions based upon flawed human training data.

An inherent issue of ADM is its lack of transparency. The resulting opacity of ADM is a hot topic in the philosophy of AI and beyond (e.g., Burrell, 2016; Felzmann et al., 2019; Creel, 2020; Buckner, 2021). It is often invoked in the literature to question the trustworthiness of AI systems in high-stakes decision-making domains and to call for more insights into their operations or for stricter regulations on their use before they are being employed in such domains (Rudin, 2019; Maclure, 2021). However, several philosophers and interdisciplinary researchers argue that this response may indicate a “double standard” or a “comparative bias” because human decision-making (HDM) in these domains is equally opaque (Zerilli et al., 2019; Buckner, 2021). The thought is that people also frequently do not know and cannot provide full insights into the actual basis of their decisions but instead explain them *post hoc* with reasons that make them appear rational. (Peters, 2022) And yet, the argument continues, the trustworthiness of HDM is commonly not much challenged.

Since this skewed situation stands unquestioned, it appears rather unfair to hold ADM systems to higher standards and require them to enable or provide exhaustive, fully accurate causal accounts of their outputs.

But ADM’s still widespread lack of transparency is systemic, while the opacity of HDM is depending on the individual. That means, at least in principle, the human decision maker can be asked about his reasons, and while the human can still confabulate and make things up, there is a chance that the person answers honestly and knows the reasons for her decision. In sharp contrast, a rejected applicant cannot ask the algorithmic system why it decided against the person. And this is a crucial distinction. After all, it is important for applicants or patients to understand why their request has been rejected.

Human ressources ADM that works after strictly implemented rules may select out applicants who apparently lack the specific background, but may be equally, if not better suited for a particular position due to their broad field of experience. That being said, a human being can also overlook a potential talent – but it shouldn’t be solely up to a stoic machine to decide over the course of life of people. Yet it works that way, is cost-efficient and helps to automate HR and other vital areas like study places at high level universities and bank loans, so we need to find optimizations for these processes.

### The Equal Opacity Argument

Based on the reasonings of a „double standard” regarding the higher demands that are directed towards ADM compared with the (roughly equally flawed) HDM, the *equal opacity argument* has been developed. The argument has direct ethical implications for the debate on whether to trust ADM in highstakes domains and how to design and regulate the algorithms involved. It thus warrants close philosophical scrutiny. (Peters, 2022)

The goal here is to critically assess the *equal opacity argument* by relating it to a particular area of recent philosophical research on the nature of people’s ascriptions of mental states and reasons to themselves. While research on mindshaping has not yet been brought to bear on the debate on whether ADM and HDM are equally opaque, the claim here is that doing so is fruitful because it offers a novel and important insight for that debate. However, the equal opacity argument narrow guides ADM and HDM in an ethical questionable way. While it is obvious that not only algorithmic decision making can result in unjust decisions, but also human decision making does, it seems reasonable to demand transparency from the tools we created to support our decision making processes. The issue of the opacity of HDM doesn’t apologize to ignore intransparent and flawed ADM in any ways. Quite the contrary, machines are designed to do the jobs humans do, but better, not only with higher efficiency, but also higher reliability. Following these objections, it appears as obvious that the equal opacity argument is based on a fallacy. Hence, we should strive to optimize the quality of the available sets of raw data.

At the core, ADM is mostly about selections based upon statistical data. Better data sets equal better decision quality, so this is the first aspect of enhancement. First steps towards better data quality are already made, as data quality is of raising priority for many leading companies that heavily rely on ADM.

Socially, ADM has the potential to increase social inequality if the issue of algorithmic bias isn’t treated as a priority. The flaws of ADM might result in profound social unrest, since the tendency of disadvantages is clearly related to the blue-collar fraction of the population. If this fatal tendency persists and even expands, social unrest might be the foreseeable and avoidable result. This shows how crucial sound solutions for ADM related issues actually are.

**The Trolley Problem**

A thought experiment that has been illustrating ethical dilemmas since the 1930s is the so-called trolley problem: In it, a driverless trolley rolls toward five people who can no longer get to safety. The only way to save them would be for a human to pull a switch to divert the train to another track with only one person on it. There is no universally valid answer to the ethical dilemma that is being constructed here. Depending on their worldview, people will either try to minimize harm (i.e., switch the switch) or adhere to the ethical principle of not intentionally killing anyone (which is what would happen if you switch the switch).

Responsibility for Autonomous Cars

The Trolley Problem was intended as a purely theoretical experiment to discuss ethical principles. It is all the more astonishing that computer scientists today have to make decisions that can be compared to it. Many car manufacturers are currently developing systems that enable autonomous driving, where the driver no longer has to hold the steering wheel (level 2), no longer looks at the road (level 3) or can even sleep while driving (level 4). It is clear that such systems must be able to emulate the behavior and decisions of drivers - even in dangerous situations that could lead to accidents. An ethical dilemma here would be how an autonomous vehicle should behave when, for example, it has the choice of driving into a group of pedestrians or into a wall instead - potentially injuring the vehicle’s occupants. A human driver or rider would make such decisions instinctively in a fraction of a second - with autonomous systems, it would have to be stored in the system in the form of computer code, meaning that humans would have to think about the situation and determine a decision. Moreover, ethical values are not universal on this issue either, but depend on factors such as wealth and cultural conditioning (Maxmen, 2018). Thus, there is an urgent need for ethical guidelines, which is recognized by both regulators (BMDV, 2017) and researchers. (Geisslinger et al., 2021). In 2022, Mercedes became the world’s first car manufacturer to receive approval for autonomous driving at Level 3 - so far only in a top-of-the-range model and under narrow conditions (among others, the system only works on highways and only at a maximum speed of 60 km/ h). However, it is expected that the technology will continue to develop and will soon be in many cars. Responsibility is clearly defined: If an accident occurs while the car is driving autonomously, the manufacturer is liable (Hebermehl, 2022). To avoid the trolley problem, a random generator appears as a potentially just solution, since the system cannot meet ethically sound decisions by itself.

### Self-check questions

1. In autonomous vehicles, algorithms have to make decisions that can endanger people’s lives.

2. The first car whose driver no longer has to look at the road in some situations was approved in 2022.

3. If the data basis of algorithms does not consider the entire population equally, this is called algorithmic bias.

## Mechanisms for Implementing Responsibility in Computer Science

Even though ethical decisions are ultimately up to the individual, in practice it makes sense to establish mechanisms that regulate responsibility for technical innovations. For example, standards can be defined for an organization or company, which then only need to be discussed when the framework conditions change. Such standards can also become an important part of the self-image of an organization and its members (such as Google’s famous “Don’t be Evil”). Ideally, they help to attract new employees who share the same ethical values. However, they will then also hold the organization accountable if they feel it is not acting in accordance with the values. In the case of Google, discussion of a project to use artificial intelligence software to analyze images collected by military drones caused a stir (Brewster, 2020). Some mechanisms that help establish accountability in organizations are presented below. Similarly, there are recommendations for codes of conduct from organizations such as the GI and its counterparts, internationally, for example, the ACM’s Code of Ethics and Professional Conduct (ACM, 2018). International organizations are also working on proposals for codes of conduct and accountability mechanisms. As an example, consider ALTAI (Assessment List on Trustworthy Artificial Intelligence), which allows users to assess the trustworthiness of an artificial intelligence. The tool was developed by the European Commission’s High-Level Expert Group on AI and tests seven requirements (European Commission, 2020):

* 1. Human action and oversight
  2. Technical robustness and security
  3. Privacy and data management
  4. Transparency
  5. Diversity, non-discrimination and fairness
  6. Environment and social well-being
  7. Accountability

Large companies that are in the public eye must be mindful of how they are perceived by various groups that have a vested interest in their operations. These groups are referred to as stakeholders. Examples of stakeholders are:

* Internal stakeholders
  + Employees
  + Managers
  + Owners
* External stakeholders
  + Customers
  + Suppliers
  + Government
  + Society

In addition to laws, to which they are bound anyway, companies often define rules within the framework of corporate responsibility. According to these, they are responsible to their stakeholders as well as to the natural environment. This reflects the fact that large companies in particular bear considerable responsibility. In addition, digital corporations in particular attach great importance to their external perception, since their users can easily switch to other providers - see the example of yahoo!, which was replaced by Google as the leading search engine (The Power of Google, 2011).

### The Age of Disruption

**Disruption**

A sudden innovation that offers a cheaper or more versatile solution for a problem, hence disrupting the original market. Digitally based examples would be Uber (disruption fort he cab market) or AirBnB (disruption for the hotel market).

Mankind has entered an age of constant and fast **disruptions**. Entire markets are vaporized while novel markets emerge. As long as change is gradual, the markets can response. (Kaplan, 2015) Too fast, and chaos reigns. Humans are very experienced in adapting to changing conditions; in fact this is what we really excell at. However, naturally some individuals are more capable of adapting than others. Thus, the resulting inequality will not only always remain, but increase, which creates winners and losers. (ibid.) AI will go on to revolutionize industries by making production processes unparalleled efficient. The resulting disruptive effects will go much deeper than simply annihilating occupations. These organizational and process improvements often make obsolete not only jobs but skills. (ibid.)

Where will these tendencies become tangible the first time? The technology to operate self-driving trucks is available today and can be retrofitted to existing fleets at very reasonable costs. (Kaplan, 2015) Trucks outfitted with such technology can „see” in all directions instead of mostly just straight ahead, drive in complete darkness or blackout conditions, and instantly share information about road conditions, nearby risks, and their own inventions. (ibid.)

For most jobs, robot state-of-the-art is still inferior to human labour in cost and performance, and advanced robotics has been a small and unprofitable business. (Moravec, 2000) There are a few exceptions in Japan, where manufacturing companies, anticipating a labor shortage in an aging population, have purchased many robots to familiarize themselves with the technology for the future. (ibid.) Another subject of automation might sound a little surprising: Sex workers. You’d think prostitution might be a job requiring a human touch. (ibid.) But also this premise is going to fade away sooner or later. And the needed shift of paradigm is already in the making. This shift away from prostitution offers several advantages. First of all it may spare countless women to do this shady job. Second it avoids legal issues. Roxxy is a female sex robot that can be highly customized and also uses AI for lifelike conversations.According to the company, „Roxxxy can carry on a discussion and expresses her love to you. She can talk, listen and feel your touch.”

(www.truecompanion.com) This is state of the art in 2023. We can only speculate how far this particular industry will go in simulating human beings. The Turing test might turn out as an easy task, routinely achieved by the representants of this industry. At the very least, ethics call for a clear distinction between human beings and humanoid robots, something that also must be reflected by the legal state of the respective entity.

Watson, a self-learning universal AI system, can sift through an equivalent of about one million books or roughly 200 million pages of data, and analyze this information and provide precise responses in less than three seconds. (Kaplan, 2015) Famous for recognizing breast cancer much more reliably than a human doctor can, this achievement is a testimony of the supreme pattern recognition artificial agents can provide. Watson will evolve into a versatile and valuable tool in the physician’s decision making process.

Excess workers and obsolete skills are a by-product of accelerating economic progress just as surely as greenhouse gases are, and the potential damage to our global labor ecosystem deserves a level of attention comparable to that of climate change. (Kaplan, 2015)

The degree of disruption caused by automation, carried out by advanced artificial intelligence, will be outstanding and has already started to lead humanity into a new era. Eventually the era of radical abundance, as the title of Eric Drexler’s book from 2014 suggests. (Drexler, 2014) Automation is taking grips on human affairs in a sneaking, yet ever broader way. The influence of automated processes driven by AI is increasing on multiple layers, combining services to most of our needs. Every smart phone offers a multitude of functions: email, social media, banking, navigation, and speech recognition services like Siri, to name a few. Two decades ago, around the year 2000, this was still far away – material of near-future science fiction scenarios. The half-life period of futuristic visions before becoming a reality is shrinking with ever-increasing momentum, and the realization of those visions changes society as well as the human self model faster than we can reflect on it. This alone explains fears of overlording scenarios, carried out by technology.

What are the next steps and changes we can expect from automation? Commercial incentives will make industrial strength AI ubiquitous, embedding cheap smartness into all that we make. We should be clear about the fact that this use of artificial brain power is merely the natural progression of mankind’s tendency to create protheses for its physical and now also mental functions. With the advent of automation and particularly services like Amazon, Uber or the rise of AI-driven high frequency trading, we get a fractured, nevertheless pretty vivid foreshadowing of what we are facing, given that the automation trend will not slow down: traditional businesses are widely dying while new ways of distribution and disruptive solutions for organizational problems emerge. The employees of this future need to remain ever adapting to these so quickly changing working environments.

This appears to pose one of the biggest (if not the most urgent) issues as mankind is in no way prepared for this rapid rate of change. We are not overwhelmed with innovations in their true sense though; the key word in this context is re-organization. As machines are inherently superior to us regarding organization principles, the rise to dominance that has already been set up becomes not only understandable but predictable. Electronic minds will grow to economic strength and eventually independence. But a bigger payoff will come when we start inventing new kinds of intelligences, and entirely new ways of thinking. (ibid.) By this we will be able to enhance human intelligence externally, by non-invasive augmentation. But unfortunately, our knowledge and understanding about the matter is limited. We don’t know what the full taxonomy of intelligence is right now. (ibid.) While machines are already replacing manpower in many areas, this tendency will strengthen and expand, as well as the wide fields of cognitive skills that will be copied and mastered by our artificial prodigy.

### Self-check questions

Why is it important to define mechanisms for implementing responsibility in organizations?

Saves time and energy by avoiding repetitive discussions. Stakeholders increasingly value sustainable action.

## Summary

Questions about responsibility and the ethically correct course of action are an integral part of human life. People have the right to reject assignments they consider unethical and the duty to question their actions from an ethical point of view. Computer scientists have to deal with ethical and moral issues in particular - also because their stakeholders are increasingly paying attention to them. Through modern technology such as ICT, this responsibility now extends to all of humanity and potentially future generations, as can be seen not only in the example of algorithms making decisions. Hans Jonas’ ethics of responsibility takes up this idea and updates Kant’s categorical imperative for a technological world. The GI has written helpful guidelines for computer scientists in German-speaking countries. Similar mechanisms for implementing responsibility and sustainability are an important tool in companies and organizations.