SOCIAL IMPACT OF DIGITAL TECHNOLOGIES EMPLOYED BY COUNTRIES IN THE WAKE OF THE COVID-19 PANDEMIC

Škavić, Fran

University of Zagreb

Faculty of Economics and Business

Master in Managerial Informatics

SOCIAL IMPACT OF DIGITAL TECHNOLOGIES EMPLOYED BY COUNTRIES IN THE WAKE OF THE COVID-19 PANDEMIC

Master thesis

Fran Škavić

Zagreb, June, 2020.

University of Zagreb

Faculty of Economics and Business

Master in Managerial Informatics

SOCIAL IMPACT OF DIGITAL TECHNOLOGIES EMPLOYED BY COUNTRIES IN THE WAKE OF THE COVID-19 PANDEMIC

Master thesis

Fran Škavić, 0066231865

Mentor: Mario Spremić, PhD

Zagreb, June, 2020.

Statement on Academic Integrity

I hereby declare and confirm that the final thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.
I declare that no part of the work has been written in an unauthorized manner, i.e., it is not transcribed from the non-cited work, and that no part of the work infringes any of the copyrights.
I also declare that no part of the work has been used for any other work in any other higher education, scientific or educational institution.

With this signature I confirm that in preparing this thesis have complied fully with the Code of Ethics of the University of Zagreb.

Student signature ______________________

Table of contents

ABSTRACT

Near the end of 2019, several worrying cases of pneumonia sprung up in Hubei province, China. Doctors immediately started investigating the novel cases of unknown etiology and notified the local CDC. Soon after, Chinese authorities informed the WHO which alarmed all other countries. The culprit for these novel cases of pneumonia was found to be a coronavirus classified as SARS-CoV-2. In just three months, the virus managed to spread across most of the world's countries and the outbreak was officially classified as a pandemic. Therefore, each country had to form a plan of actions and measures serving to curtail the spread of the virus. Most countries leveraged digital technologies in their quest to flatten the curve. However, some implementations of digital technology infiltrated the area of personal privacy in varying degrees. Therefore, the aim of this paper is to give some notable examples of country-specific measures and analyse their ethical and societal impact.

Keywords: Covid-19 pandemic, privacy, surveillance, security

1. INTRODUCTION

1.1. Topic and Goal of Master Thesis

At the present time of writing, humanity is facing a novel common enemy which has seemingly stopped most of the world in its tracks. This common enemy is the latest pandemic caused by the SARS-CoV-2 coronavirus, it has spread rapidly across the globe since first cases appeared in Wuhan, China near the end of 2019. Due to its highly contagious and detrimental nature, human contact had to be limited and controlled. Therefore, as the virus proliferated among the world's population, different countries instated various measures and techniques to curtail its spread.

More often than not, these actions heavily relied on the use of digital technologies. In order to gain more insight into data collected from these efforts, these same countries had to digitally transform their systems. The extent and success of digital efforts will be investigated according to the MIT digital transformation methodology. Therefore, the goal of this thesis is to present an overview of such governmental initiatives employed by countries across the world, with an emphasis on the social and ethical impact thereof.

Furthermore, it is of interest to see how these approaches varied from country to country and to what extent countries leveraged their existing capabilities. Governmental activities will be examined across different categories of digital technology implementation, the most important of which is contact tracing. Finally, the work will also touch upon broader monitoring endeavours employed by some countries.

1.2. Data Sources and Methodology

The great majority of literature data used for writing this paper was retrieved from online sources. They consist of scientific papers, mainly peer-reviewed research papers, review papers and conference papers, with the addition of newspaper articles where scientific literature is not available due to the novel nature of the current pandemic. Data from these sources will be qualitatively analysed using methods of induction and deduction before synthesising the findings into a comprehensive overview. Finally, MIT's framework for digital companies will be employed for categorising and explaining digital transformation efforts of different countries around the world.

1.3. Content and Structure of the Thesis

The thesis spans across seven chapters, starting with an introductory chapter which contains the topic and goal of the master thesis, information about data sources and methodology, as well as the content and structure of the paper.

After the introductory chapter, this thesis continues with three literature chapters that aim to inform the reader about the broader context of the paper in addition to showcasing real-world applications of discussed technologies. The first literature chapter concerns digital technologies, specifically basic and emerging technologies, as well as the closely related topic of digital transformation.

Contrary to focusing solely on the benefits of digital technologies, the subsequent chapter features social and ethical issues connected to the use of digital technologies. The main idea of this section is to portray the problematic of moral dichotomy in employing digital technologies.

After social and ethical issues have been detailed, the last literature chapter deals with the characteristics of the Covid-19 pandemic. Specifically, a history of previous coronavirus outbreaks and the chronological evolvement of Covid-19 into a pandemic.

After concluding the literature overview, it is time to move on with the central part of the thesis. This part presents various governmental efforts for curtailing the spread of Covid-19 employed by countries around the world, along with a summation of their digital transformation using the MIT digital company framework.

Chapter six is reserved for analysing research results from chapter five, with a keen focus on depicting specific social issues. Following the analysis comes the seventh, final, chapter which concludes the paper with closing remarks and suggestions for further research.

2. LITERATURE REVIEW OF DIGITAL TECHNOLOGIES

Digital technologies have become ubiquitous in our everyday lives, both personal and professional. Today the credo is 'digital or die', which means that companies cannot afford to be digitally impaired or live off their old glory. This also brings with it the fact that no company is safe from competitors, not even big, well-established corporations. Newcomers from a variety of fields are leveraging digital technologies to succeed in the marketplace. Their strength lies in the ability to offer better services at a fraction of the cost, while also personalising content and thus, engaging with their customers. The lifeblood of this new economy is data, companies collect, analyse and use customer data to personalise their offering and improve service. Seeing the role digital technologies play in everyday life of citizens and recognising their potential for a variety of uses, governments worldwide have begun to increasingly implement them to supplement various public initiatives. Furthermore, some areas of the public sector even completely digitally transformed.

Digital technologies can be classified along two categories as presented in Spremić (2017 a). Those categories are primary and secondary, or basic and emerging digital technologies. The author describes basic digital technologies as mature ones which are already commonplace in almost every business today. They include mobile technologies, social networks, cloud computing, big data and sensors coupled by Internet of Things (IoT). In contrast, emerging digital technologies have the potential to become ubiquitous across businesses, but are still to improve and evolve. Some emerging technologies include wearable technology, robotics, cognitive technologies such as artificial intelligence (AI) and facial and speech recognition. Due to the rapid pace of technological improvement, some of the aforementioned emerging technologies are rapidly becoming established across businesses.

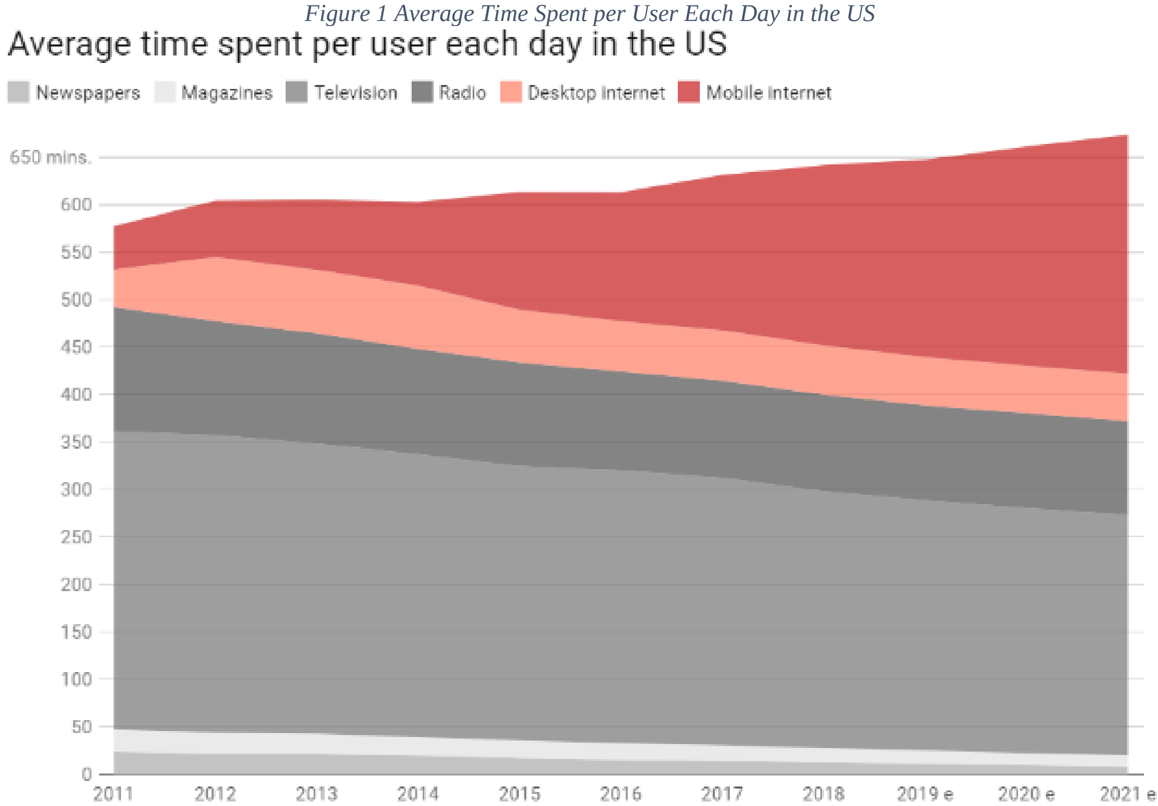
2.1. Basic Digital Technologies

Literature overview of basic digital technologies follows a three-part structure. The first part focuses on defining the term in question. The second part depicts noteworthy business and uses of the selected technology, and the final part covers its public sector use. Regarding specific technologies, the subchapter begins with an examination of mobile technologies and social networks - the two most common and visible digital technologies in everyday life of most people. Next, we move on with two equally prominent, yet invisible, technologies - cloud computing and big data, before tackling the final basic technology - sensors and Internet of Things.

2.1.1. Mobile Technologies

The staple of modern mobile technology is the smartphone. Gartner (N.D. a) defines a smartphone as *"a mobile phone which primarily runs an Android or iOS operating system and thus supports installation and operation of applications."* Contrary to traditional mobile phones, smartphones host a variety of sensors such as a proximity sensor, gyroscope and accelerometer along with wireless communication protocols like Bluetooth, GPS and Wi-Fi. Bluetooth serves to establish wireless connections with other devices and exchange data. GPS enables precise global positioning and navigation and Wi-Fi wirelessly connects the device to an internet network or connects two devices to exchange data. The cooperative manner of applications and sensors allows for endless possibilities in terms of smartphone use. In terms of usage statistics, over 3 billion people owned a smartphone in 2019 according to O'dea (2020). While over 1.5 billion smartphones were sold to end-users around the globe according to a research from Gartner (2020). When we observe statistical data about smartphone usage in the United States, we can see a rising trend in mobile internet usage. On the other hand, traditional media outlets such as television, radio, newspapers and magazines are proportionally declining. However, it is not only traditional media which is deteriorating in popularity, from the image below it is evident that desktop internet usage is stagnating as well.

Figure 1 Average Time Spent per User Each Day in the US



Retrieved from: https://www.vox.com/recode/2020/1/6/21048116/tech-companies-time-well-spent-mobile-phone-usage-data (accessed: 3 March 2020)

As smartphones became a fixture of modern life, their functionality became even more varied and useful. So much so that people who do not own such devices become severely limited in their ability to participate in today's societal and economic activities. In the Global Mobile Consumer Survey from Deloitte, author Wigginton (2018) states that one-third of their respondents regularly use smartphones to pay for products. Between 10 and 20 per cent of users are using smartphones to pay for services or public transport and between 13 and 30 per cent of people use their phones to make in-store payments.

These figures are even higher in China due to the prevalence of so-called 'super apps'. Such mobile applications feature a host of functionality which are almost universally used in daily life. One such application is WeChat. It was launched in 2011 by the Chinese company Tencent Holdings. Throughout the years it developed from a simple messaging app into an indispensable platform for daily life. In business, WeChat is even preferred to email communication, and the ban of American social media sites allowed WeChat's social feature Moments to dominate that field as well. However, one of the three main distinguishing features can best be observed in an article on the subject, written by Kharpal (2019). The author writes: *"From major supermarkets to the smallest of street vendors and taxis, you can pay for things with WeChat almost anywhere in China. As long as you have a Chinese bank account, you can link that to WeChat."* Whether a person is paying for products or services in person or online, WeChat Pay is almost always an option. When combined with instant money transfers via the messaging function, it is no wonder the app managed to acquire over 1.2 billion active users. The second distinguishing feature of WeChat is the addition of 'mini-programs'. Mini programs are sub-applications within the app which can be used for almost anything, including watching videos, listening to music, renting bikes, hailing rides, rating restaurants, shopping for various products, finding a charging station for your electric car, buying public transport passes and a myriad of other things, all without leaving the app. In addition to private and business uses, WeChat is increasingly used in the public sphere as well. For example, The Straits Times (2017) reports that a court in Beijing has opened an account to allow litigants to contact judges and thereby receive status updates on their cases. Judges are required to reply within 24 hours to litigants' questions, thus laying the grounds for a transparent and expedient judiciary system.

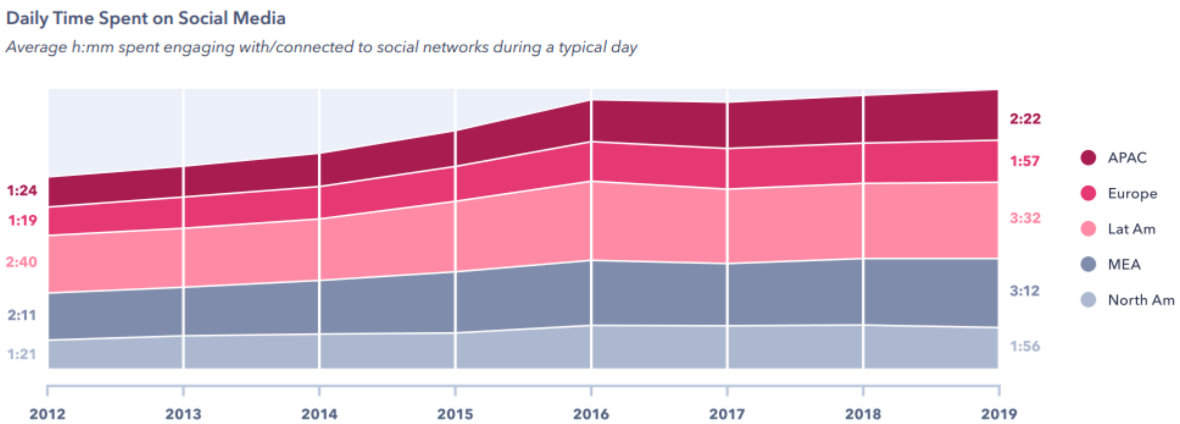
The Chinese government is not alone in the quest for achieving a mobile-friendly government as countries around the world are increasingly leveraging mobile technologies. The book M-Government: Mobile Technologies for Responsive Governments and Connected Societies by

OECD (2011) tackles this topic in great detail. Although a somewhat dated publication (2011) it is still an influential work because it provides a comprehensive overview of the subject along with some compelling examples. Two most notable examples are outlined in chapter two; they are the SMS Judicial Information System in Turkey and the Mobile ID system in Estonia. The SMS Judicial Information System began as a rudimentary service which enabled lawyers and citizens to receive messages with legal information such as dates of court hearings, information about ongoing cases and current cases against them. Since its inception, this basic service grew into a sophisticated platform which allows users to electronically sign paperwork and reach most courts when requesting copies of personal data. On the other hand, Estonia's Mobile ID service serves a different purpose. It is a secure system for digitally identifying internet users. However, there is a prerequisite for using the service, users must acquire a special SIM card and activate it with an Estonian ID card. Once activated, the Mobile ID certificate is ready for use. It can also be used for authenticating users across various compatible websites which allows for a prompt and secure login. Furthermore, since 2011 the system was also used for voting.

2.1.2. Social Networks

Mobile technologies and social networks are two of the most pervasive technologies in everyday life. Furthermore, the two are closely interlinked. Almost every smartphone user has at least one social media account, amounting to 3.76 billion active mobile social media users as of April of 2020 according to Clement (2020). These same users spend an average of two and a half hours on social networking sites each day, with even higher percentages observed in the younger demographic. Moreover, users are spending increasingly more time on social networking sites as is visible from the image below.

Figure 2 Daily Time Spent on Social Media



Retrieved from: www.globalwebindex.com (accessed 7 March 2020)

This uptake in usage can partly be attributed to the evolution of social networking services which evolved into sophisticated platforms for entertainment as well as commerce. Despite being a reasonably new phenomenon, social commerce has become increasingly prominent in recent years. Researcher Lai (2010) defines the term in her work on social commerce as *"the use of social media, in the context of e-commerce, to assist with buying and selling products and services online. It evokes the fusion of two big digital trends, e-commerce and social media."* In effect, around 28% of customers report making a purchase based on social media advertising, while 24% made a purchase based on recommendations or comments on social networking sites according to the Global Web Index report (2019).

Therefore, most companies today strive to on leverage social networks to increase productivity and add value for their customers. However, only a small number of companies manage to do so. Two noteworthy examples come from Domino's Pizza and KLM Royal Dutch Airlines. Domino's Pizza is one of the most digitally advanced companies in the world and is continuously experimenting with new ways to utilise technology. Their "Pizza Anyware" campaign offers users the possibility to order a pizza through Facebook's Messenger, by sending a Tweet with the hashtag #Easyorder or even through the regular Messaging app on any device by sending a pizza-shaped emoticon. On the other hand, KLM Airlines focuses solely on Facebook's Messenger. Through it, the company sends personalised flight information to their customers. Some of the functionality also includes prompt customer service, flight delay notifications and even automatic flight rescheduling along with sending an electronic boarding pass.

However, social networks are not only utilised by individuals and companies; governmental efforts in the sphere of social technologies have been swelling as well. Most of these efforts only feature one-way communication, whereby the national agency in question reports on their current activities. This is laudable as it increases transparency, but does little for citizen engagement. Nevertheless, there are examples of government agencies which engage their audience. In the working paper on Social Media Use by Governments, OECD (2014) provides two such examples. The first concerns the Chilean government, and the other Spanish police. Chile's social media approach is uncommon, but praiseworthy, as the country engages stakeholders to co-create strategies and critical documents. Their e-government strategy cycled through several public iterations before reaching its final state in 2012. This focus on engagement was also a crucial cog for the Spanish national police which committed to using social networking sites from very early on, starting with campaigns in 2009. Their efforts are multichannel, encompassing Facebook, YouTube and Twitter. In communicating with their followers, they rely on sending genuine, content-rich messages written in "plain" language, sometimes even humorous. The content of their posts is not tied to governmental propaganda, but topics of interest to the general public. This clear communication and topic curation have proven to be successful for garnering a large following, which in turn helped the police in certain mission-critical activities.

2.1.3. Cloud Computing

As opposed to mobile and social technologies, cloud computing is not so visibly present in everyday lives of most people, but still it plays a substantial role in the backdrop of almost every service people use. By definition of the National Institute of Standards and Technology (NIST) (2011), Cloud computing can be defined as *“a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”* In their book on the subject, authors Wang et al. (2013) identified the following features as central in utilising cloud computing:

- Agility – allows rapid and inexpensive re-provisioning of resources.
- Location Independence – stored data can be accessed from anywhere in the world.
- Multi-Tenancy – stored data is shared among a large pool of users.
- Reliability – dependable access to computation power and stored data.
- Scalability – dynamic data provisioning helps avoid bottlenecks.
- Maintenance – responsibility for maintaining and upgrading the platform is performed by service providers rather than the company.

Therefore, the main benefit of utilising cloud computing as opposed to in-house systems lies in eliminating unnecessary overheads. In a single term, cloud computing boasts the principle of "Everything as a service", abbreviated XaaS. Three main service delivery modes stem from this credo: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Additionally, there is also Database as a Service (DBaaS) which is present in some literature sources and absent in others. The degree of user freedom and complexity of interactions vary from very limited in the case of SaaS, moderately limited in PaaS and lenient when utilising IaaS. There are three leading cloud computing service providers according to

Marinescu (2018): Amazon, Google and Microsoft. Today Amazon dominates the cloud computing landscape with its Amazon Web Services (AWS) platform, focusing on providing IaaS which it pioneered in 2006. Google focuses its efforts on SaaS and PaaS, while Microsoft mostly provides PaaS. Additionally, Amazon and Oracle offer DBaaS.

Due to the plethora of advantages cloud computing has over traditional storage and computing, it is a challenging task to find a company which does not rely on it. Companies like Netflix, Samsung, Adobe, Lionsgate and Pfizer, to name a few, rely on AWS to support their operations in a customisable and affordable way. Other companies such as Boeing, Pixar, Xerox, 3M, Mazda, Audi and LG chose Microsoft's Azure cloud platform. While Google's cloud services are the platform of choice for PayPal, The Home Depot, Target and HSBC. In fact, many companies digitally transformed their operations thanks to the cloud. One example is Netflix which transformed its operations from a physical video rental business into the multimedia streaming giant it is today.

Cloud computing is transforming the public sector as well, many cities are storing data on the cloud and some are even employing cloud computing. Examples from Croatia include cities of Kutina and Dubrovnik. Kutina has digitalised its operations and implemented cloud computing back in 2018, while Dubrovnik went further with its Smart City initiative. Other public sector uses from around the world are outlined in the research on Cloud Computing Utilization in the Public Sector written by Abu-Shanab and Estatiya (2017). The first use case concerns management of laboratories where a cloud storage module digitalised lab results which sped up queries in a confidential manner. Second, Integrated Library Management Software (ILMS) is being increasingly discarded for cloud-based software which allows greater privacy, security and scalability at a lower cost. Next, federal areas and the Army already benefit from combining CRM software and social networks by increasing the size of recruiting. Finally, education and healthcare are two areas where cloud computing can have the greatest impact. E-learning and Telecare projects are already being developed by several countries with a hope of allowing instant, stable and secure access to a vast repository of data.

2.1.4. Big Data

The historical definition of big data described it as data which is so large, fast and complex that it is impossible to process it using traditional methods. Throughout the years, big data became widely used and researched, thus its definition evolved. Today, Garner (N.D. b) describes big data as *"high-volume, high-velocity and/or high-variety information assets that demand cost-*

effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation." These three Vs: volume, velocity and variety establish a comprehensive definition by shattering the myth that big data is solely about volume as previously thought. Still, volume is the primary attribute, more and more the volume of big data is measured in petabytes and exabytes rather than terabytes. This is in part due to greater variety of unstructured, semi-structured and structured data which is increasingly stored and analysed. Companies are collecting data by tracking user's digital movements, registering clicks, analysing uploaded textual, photographic or video content, and much more. The other contributing factor responsible for such magnanimous volume is its velocity. Clickstream, sensor and streaming data is generated blazingly fast. All of this data has to be stored for dissemination in order to reap the benefits of collecting it. However, as companies utilise big data analytics, quick knowledge discovery from vast amounts of datasets allows them to offer exponentially better service for their customers.

A remarkable example of big data analytics in action can be observed from the video streaming giant Netflix. On account of collecting and analysing data from more than 150 million subscribers, the company is able to successfully curate personalised recommendations to each one of their subscribers. The extent of this feat is best observed during a marketing campaign for the 'House of Cards' series. Netflix made ten different trailers for the series according to the most prominent trends among viewers. In their post about the topic, Selerity SAS (2019) explained how this worked in practice: *"If the user predominantly watched TV shows centred on women, they would get a trailer focused on the female characters. However, if the user predominantly watched content directed by David Finch, they would have gotten a trailer that focused the trailer on him. Netflix did not have to spend too much time and resources on marketing because they already knew how many people would be interested in it and what would incentivise them to tune in."* Another noteworthy example of big data analytics can be observed at airports. As reported in the Harvard Business Review by Mcaffe and Brynjolfsson (2014), airports previously relied on pilot reports for ETAs which were unreliable to say the least. About 10% of flights had at least a 10-minute gap, while 30% of flights had a gap of at least 5 minutes, resulting in bottlenecks causing a domino effect of further delays. However, since airports started relying on RightETA from PASSUR Aerospace, ETAs have become precise within seconds. The system collects and analyses real-time weather data, flight schedules, sensor data and current aeroplane position data to give airports a precise window of time during which aeroplanes are expected to land.

Contrary to business goals like predicting customer behaviour and developing a competitive edge, governmental uses of big data focus mostly on providing sustainable solutions which enhance transparency and balance social communities. For example, the United States developed a massive, but scalable, infrastructure to manage real-time streaming data called InfoSphere in 2002. This initiative was followed by mass digitalisation and publishing of transportation, economy, health care, human services and education related data in 2009 which were published on Data.gov in an effort to increase transparency and accountability. Likewise, since 2012, the European Union performed a similar feat with its Digital Agenda for Europe. Its goal was to create a vast pool of knowledge concerning member states of the EU. Lastly, besides storing and publishing data, governments also utilise big data analytics for monitoring inflation, detecting fraud, identifying possible terrorist threats or cyberattacks and aiding emergency responders.

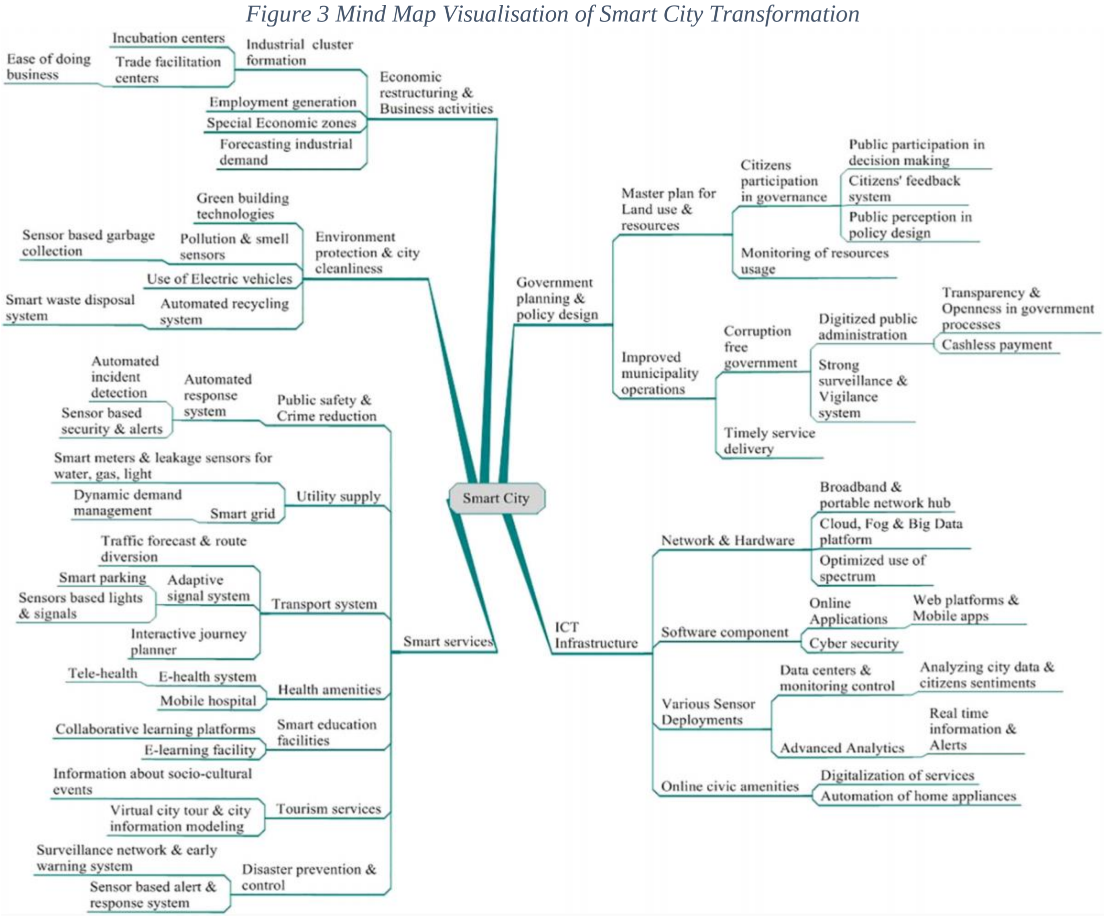
2.1.5. Sensors Coupled with Internet of Things (IoT)

Sensors and Internet of Things are two basic digital technologies which are complementary in practice. In their conference paper on recent trends concerning IoT applications, researchers Saha, Mandal and Sinha (2017) presented their definition of IoT and the role of sensors as follows: "*Internet of Things (IoT) is a network of networks of physical objects that may include vehicles, buildings, energetics, construction equipment, and health monitoring devices. Such a network utilises electronic devices such as sensors and actuators to fulfil its purpose of exchanging and updating information, and hence, negotiate to achieve optimum performance by the overall system.*" These sensors and devices communicate among themselves without human interference using Internet Protocol (IP) connectivity. Results of their interaction serve to aid humans or Artificial Intelligence in decision-making. Since sensors and IoT technology have been available for a relatively long time, the scope of their implementation is vast. As researchers Singh and Singh (2015) stated in their work, IoT technology facilitates smarter analytics because the use of more inter-connected devices draws with it more valuable data to analyse. Similarly, placement of sensors within a number of devices to monitor their overall health in real time lowers maintenance costs and increases productivity. Sensors are also critical for managing inventory, in fact, the first use of this technology was in Carnegie Melon University for monitoring the number and temperature of Coca-Cola bottles in their vending machine. Finally, all modalities of transportation have greatly benefited from this technology as well, specifically in terms of vehicle diagnostics and real-time weather and traffic condition reporting, resulting in safer travel.

Concrete examples of IoT implementation in business are abundant, however one of the landmark examples is that of General Electric (GE). GE shifted its operations from producing large industrial equipment to providing monitoring services through its industrial digital platform called Predix. Starting from 2012 GE has completely digitally transformed its operations. In their new business model focused around the Predix platform, GE is collecting data from over 100 million sensors to provide greater insight into the health of jet turbines, oil wells, pipelines and various other infrastructure and devices. Other manufacturing companies like Audi, Harley Davidson and Airbus also rely on IoT in their new digitised manufacturing operations. For instance, in Harley Davidson's new production facility, every machine is a connected device with all variables continuously monitored, allowing for predictive instead of reactive maintenance as well as much faster production. The end result is a $200 million reduction in operating cost and a shortened order fulfilment cycle from 21 days to six hours.

This technology has great potential in the public sector as well. In recent years, discussions on IoT use in the public sector mostly rely on the concept of 'smart cities'. According to a publication by the European Parliament, a smart city is defined as *"a place where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefits of its inhabitants and businesses."* Therefore, the focal purpose of smart cities is to improve the lives of citizens, environmental efficiency and security. This is done though collecting data from thousands of IoT devices which monitor everything from traffic conditions, parking spots, air pollution, water management systems and a variety of other areas within a city. A mind map containing most features of an optimal smart city is outlined in the page below.

Figure 3 Mind Map Visualisation of Smart City Transformation



Retrieved from: Kumar et al. 2018 (accessed 30 April 2020)

In Croatia, the most digitally advanced city is Dubrovnik. Various sensors are placed across the city, serving various purposes. In-ground parking sensors notify users about available parking spots, various beacons navigate tourists to the city's top attractions and sensors monitor real-time humidity of the soil to irrigate only when necessary. Additionally, various cameras have been placed to combat overcrowding in some regions of the city. Infrastructure is constantly improving, and so is the scope of technological features, but so far, results have been very encouraging. So much so that over 100 Croatian cities decided to follow suite and are planning to implement similar solutions.

2.2. Emerging Digital Technologies

Literature overview of emerging digital technologies follows the same three-part structure as contained in the subchapter of basic digital technologies. The first part focuses on defining the term in question. The second part depicts noteworthy business uses of the selected technology, and the final part covers its public sector use. Regarding specific technologies, this subchapter begins with an examination of wearable technology, moving on with robotic, then artificial intelligence and finally, facial and speech recognition.

2.2.1. Wearable Technology

The first iteration of emerging technology is Wearable technology, and it is an evolving application of sensor and IoT technologies detailed in the previous subchapter. Since 2014 onward wearable devices, or wearables, have become more readily available to consumers. As interest in these devices rose, their form and functionality became more varied and elaborate. Likewise, they garnered sizeable curiosity from the research community as well. By definition of Gao et al. (2016), "*Wearable electronics are devices that can be worn or mated with human skin to continuously and closely monitor an individual's activities, without interrupting or limiting the user's motions.*" As outlined in the work of Hussein (2015), modern-day wearables host a variety of sensors depending on their application such as an accelerometer, infrared sensor, glucose sensor, humidity and temperature sensor. In addition to monitoring human activities, wearables wirelessly transmit results to another device, usually a smartphone. Vice-versa, smartphones can also send information to the device. Wireless communication usually occurs over Bluetooth or Wi-Fi. Therefore, their form varies depending on the function they serve, from fashionable clothing, wristbands, wristwatches, belts, head-mounted displays, to glasses and earpieces. Most wearable technology implementation efforts today mostly pertain to medical applications and personal wellbeing, while other evolving domains include construction, monitoring social interactions, agriculture, navigation and safety.

In the commercial sector, personal wellbeing wearables have been dominating the market for the last couple of years. Most consumers were introduced to fitness wearables in 2009 through Fitbit. Beginning as a wireless clip that latches on clothes and evolving into the signature wristband known today, it counted steps, calculated calorie output and monitored sleep quality. Today, similar devices are manufactured by various other companies including Garmin, Apple, Xiaomi, Motiv and Bellabeat. Either designed as a wristband, wristwatch or smart jewellery, these devices monitor users' activity levels, sleep cycle, menstrual cycle, hydration and even stress levels with a respectable degree of accuracy. Data produced from such devices has become sought after in the insurance industry. For example, some life insurance plans offer customers discounts if they share data from their Fitbit. Other iterations of wearable technology include interesting examples such as the WeWalk cane, Smart Belt Pro, Athos and Apollo bracelet. WeWalk is a smart walking cane for visually impaired people. It detects obstacles, provides turn-by-turn navigation and listens to voice commands. On the other hand, Smart Belt Pro is a belt which relies on various sensors to conduct fall risk assessment and recommend exercises to improve coordination, thereby minimising the risk of falling. Additionally, the belt also serves as a fitness tracker. Next, Athos is a company specialising in producing smart training clothes equipped with sensors which monitor the strain on muscles in athletes, allowing the app to coach them accordingly in order for users to reach their full athletic potential. Finally, the Apollo bracelet focuses on stress alleviation using vibrational waves. The device sends specific vibrational patterns through the motor inside the armband thereby stimulating the parasympathetic nervous system.

When it comes to public sector implementations, examples are mostly concentrated around future use in healthcare. Researchers Mahajan et al. (2020) argue that diagnostic wearables could drastically lower costs of patient care in addition to providing troves of data about various diseases along with allowing personalised treatment for individuals. Furthermore, other researchers propose remote health monitoring using wearable technology to gain a deeper insight into health conditions of senior individuals. One such proposed system detailed in the work of Al-khafajiy Mohammed et al. (2019) is called 'SW-SHMS' and it would utilise wearable technology paired with a smartphone to measure vital signs of patients including blood oxygen saturation, heart rate and skin temperature. Sensory data would be transmitted in real time to the hospital's cloud using mobile technologies. Data would then be analysed and abnormal conditions recorded for doctors to review. If the condition is cause for concern, the patient would be notified immediately and encouraged to visit the hospital for further diagnosis. Aside from future uses in healthcare, wearable technologies are already used in the justice system. For example, police forces around the world are increasingly adopting body cameras. In the United States, wearable cameras were a response to accusations on racially charged officers and also false citizen complaints. Certainly in the future as wearable technologies evolve so will their scope of application.

2.2.2. Robotics

Similarly, the field of robotics has seen a marked uptake in implementation following its evolution. It is a wide field of knowledge with continually increasing applications. In the book Introduction to Robotics, author Niku (2011) defined robotics as *"the art, knowledge base, and know-how of designing, applying, and using robots in human endeavours."* While the definition of robots is given in Guizzo (2018 a), defining them as *"autonomous machines capable of sensing their environment, carrying out computations to make decisions, and performing actions in the real world."* Serving as an instrument for human endeavours, robots are designed to go places where humans cannot and see things we would be unable to see. This includes hazardous environments such as radiation, ocean bottoms, space and extremely high or low temperatures. Moreover, robots are far more accurate than humans and can work continuously without becoming fatigued or bored. Finally, when equipped with artificial intelligence, robots can also be more skilled than humans in a specific area of application. Owing to a wide variety of applications, there are many types of robots. Certain types are presented below according to a classification by Guizzo (2018 b):

- **Aerospace robots –** a broad category which includes everything from flying robots mimicking birds to NASA's Robonaut Mars rover.
- **Consumer robots –** functioning as an entertaining companion or helpful hand. Examples include the robot dog Aibo, Roomba vacuum cleaner and various other AI powered robotic kits and toys.
- **Disaster response robots –** perform jobs which are too dangerous for humans. An example is Japanese use of the Packbot in 2011 to determine the extent of damage at the Fukoshima nuclear station.
- **Drones –** or unmanned aerial vehicles (UAVs) come in various shapes and sizes with different levels of autonomy. Examples include commercially available drones such as DJI Phantom as well as military use drones like Global Hawk.
- **Humanoid robots –** are designed to mimic the shape, movement and gestures of humans. Perhaps the most well-known humanoid robot is Honda's Asimo.
- **Industrial robots –** ubiquitous across factories and warehouses across the globe, such robots serve different purposes from assembling and products to delivering them across the facility.
- **Medical robots –** include surgical robots, bionic prostheses, robotic exoskeletons and telepresence robots.
- **Military robots –** various robotic devices aiding military missions. Examples include PackBots for defusing IED devices on the ground, Predator drones for surveillance and suppression in the air and the AQUA2 for dive assistance and underwater monitoring.
- **Self-driving vehicles –** autonomous vehicles which can be used for transporting people in controlled areas or transport supplies from one point to another.

Regarding the use of robotics in business, most pertain to manufacturing and logistics. Manufacturing robots perform anything from food packaging, arc and spot welding, steel cutting, painting, palletising, die casting, injection moulding to nuclear waste handling. Most also work in collaboration with other robots, but a new generation of collaborative robots or cobots is able to work alongside people. Cobots are also used for logistic purposes inside warehouses. Croatian companies Tokić, Atlantic and Orbico already use autonomous warehouse robots produced by Gideon Brothers in their day-to-day operations. These robots are equipped with various sensing devices using which they are able to plot their surroundings and navigate them accordingly. Additionally, sensors serve to detect humans and stop the vehicle if necessary, thereby eliminating the need for special road markings to guide the robot. Another increasingly important technological trend in robotics is pointed out in Gartner's top 10 strategical trends for 2020 and it is hyperautomation. Author Panetta (2019) described the essence of hyperautomation as basically automating all that can be automated. An exciting example of hyperautomation comes from a Chinese e-commerce company called JD.com. The company managed to fully automate its warehouse, employing only four people with the sole purpose of maintaining the robotic infrastructure. Their warehouse is staffed with collaborative, autonomous robots which pick, transport, package and ship products. Similar autonomous robots are also used for food delivery in controlled environments across the world. For example, a company from the United States produces autonomous food delivery robots. Such 'Starship' robots can carry items within a 6 km radius in a secure and prompt manner.

On the other hand, public sector use of robotics is quite varied. However, most cases revolve around military use. This is in part due to the fact that robots can perform tasks which are either impossible or fatal for humans and in other part, use of robotics can provide a tactical advantage over the opponent. Such example in the real world are military drones which revolutionised modern warfare. The United States relies heavily on drones to survey and eliminate enemy forces. Their latest drone, Predator C Avenger, is able to carry a variety of highly destructive bombs at altitudes over 15 km during a maximum 20 hour flight. As such it is one of the most technologically advanced drones in the world, promising to dominate the skies. However, another frontier is still largely unconquered, and underwater unmanned vehicles (UUVs) serve to turn that trend around. Unmanned submarines are the next revolutionary step in modern warfare and China is on the forefront of their development. In 2019, China unveiled their UUV called HSU-001 which, according to an article by Pike (N.D.) on the topic, has three basic missions: *"1 collecting intelligence, conducting surface search and reconnaissance; 2 reconnaissance of mines, collecting marine tactical data; 3 conducting anti-submarine warfare in coastal shallow waters."* In the future, researchers suggest that aside from their use in the military, robots will be crucial for revolutionising healthcare.

2.2.3. Artificial Intelligence (AI)

There are various definitions of artificial intelligence, however Britannica provides an encompassing one. According to the article, artificial intelligence is defined as *"the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. The term is frequently applied to the project of developing systems endowed with the intellectual processes characteristic of humans, such as the ability to reason, discover meaning, generalise, or learn from past experience."* Similarly, there are various methods for classifying AI, such as the three type classification brought forward in the article by Serokell (2020) used for the purposes of this paper. At the time of writing, all practical applications of AI pertain to the first type of narrow or weak artificial intelligence. Known as Artificial Narrow Intelligence (ANI), this type of AI is exceptionally good at performing a single, very specific task either with human supervision or completely autonomously. However, such AI cannot perform tasks outside of its narrow scope of application. The second type of AI, called Artificial General Intelligence (AGI), could do so. AGI would act similar to a human in its ability to learn, understand and perceive the world around it. Finally, the most advanced form of AI is called Artificial Superintelligence (ASI) and is best described in the work of Bostrom (2006) who described it as: *"an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom and social skills."* Despite the definition of present state AI as 'weak', it is a technology which is not only present in almost all fields of science and business, but is also pervasive in other digital technologies. This is due to its ability to analyse vast troves of data, form a conclusion and act autonomously based on the results. Therefore, it is no surprise that AI implementation spans from agriculture to zoology, covering everything in between. Its use in chatbots and image recognition are outlined below.

The first example of artificial intelligence implementation are conversational agents or chatbots. As defined by Arsenijevic and Jovic (2019), the goal of chatbots is "*to have a conversation with humans. It is desirable that access to information be as easy as possible for the person and the messaging platforms are selected as convenient platforms for people to use for daily communication."* Most people interacted with a chatbot at one point in time. Either by using a digital assistant on their phone or when contacting customer service online. Chatbots are also used in education, medicine, charity, business and entertainment. Capabilities and scope of implementation are continually increasing due to advances in natural language processing capabilities as well as machine learning. In the sphere of voice assistants this means that chatbots can now make phone calls to third parties and successfully interact with them. Specifically, Google's newest voice assistant can. If online booking is not available, the assistant can call the business in question and make reservations. The fascinating thing is that this voice assistant sounds very much like a human being, along with mimicking common conversational nuances. Aside from chatbots, AI is also profusely used for image recognition. One important use of applied image recognition is in medicine, as outlined in the work of Yeasmin (2019), AI powered medical robots can spot skin tumours more accurately and speedily than their human counterparts, diagnose MRI scans with almost 100% accuracy and draw blood as professionally as a nurse. Next, another increasingly important function of AI in medicine is its ability to quickly analyse vast troves of textual data in order to aid doctors with proper diagnosis. For example, IBM's Watson is already working alongside doctors and nurses in over 100 hospitals to diagnose patients by analysing their medical history.

Due to the ability of AI to analyse vast amounts of structured and unstructured data and act autonomously, it is increasingly used in the public sector as well. Specifically, in the justice system. One such example is a program created through a joint collaboration between the Los Angeles Police Department and UCLA called PredPol. PredPol is a predictive policing algorithm which uses three data points: crime location, crime type and crime time/date to map hotspots of high criminal behaviour. Once hotspots are determined, the algorithm plans out a patrol schedule which serves to stunt criminal behaviour. After some time, results are analysed and future actions are adjusted accordingly. Alternatively, the European Union also relies on AI to aid criminal justice efforts. Their VALCRI (Visual Analytics for Sense-Making in Criminal Intelligence and Analysis) system serves to analyse historic and actual criminal data in an unbiased way. VALCRI can quickly locate suspicious or interesting information from a number of data sets. Furthermore, its advanced search function compiles and presents various meaningful associated data about the subject in question. Lastly, VALCRI also organises large data sets in customisable thematic clusters. The final example of governmental AI implementation comes from the UK. The HART (Harm Assessment Risk Tool) is the result of a collaboration between Durham Constabulary and University of Cambridge. The central goal of this project was to foster consistency in decision making and enabling targeted interventions. As outlined by Oswald et al. (2018), the HART model is able to categorise offenders into three predicted risk groups: *"First, offenders who are predicted as likely to commit a new serious offence over the next two years are placed in the High-Risk group. Secondly, those whose forecasted offending over this same time frame will be limited to non-serious crimes are* *designated as Moderate Risk. Finally, those who are predicted to commit no new offences during the next two years are identified as Low Risk."* The importance of this model in practice is its objective and thorough classification of offenders which aids officers to adjust the tightness of restrictive measures when plotting future actions related to the offender. Criminal justice is an interesting showcase of AI application in the public sector, however, other areas in which AI can play a sizeable role also include examples from the figure below:

Figure 4 Types of Areas Suitable for AI Applications

Resource Allocation	• Administrative support is needed to speed up task completion • Inquiry response times are long due to insufficient support
Large Datasets	• Dataset is too large for employees to work with efficiently • Internal and external datasets can be combined to enhance outputs and insights • Data is highly structured with years of history
Experts Shortage	• Basic questions can be answered, freeing up time for experts • Niche issues can be learned to support experts in research
Predictable Scenario	• Situation is predictable based on historical data • Prediction will help with time-sensitive responses
Procedural	• Task is repetitive in nature • Inputs/outputs have binary answer
Diverse Data	• Data includes visual/spatial and auditory/linguistic information • Qualitative and quantitative data needs to be summarized regularly

Retrieved from: https://ash.harvard.edu/files/ash/files/artificial_intelligence_for_citizen_services.pdf (accessed 27 May 2020)

2.2.4. Facial and Speech Recognition

The final emerging technologies in this paper are facial and speech recognition. By definition from Thorat et al. (2010), a facial recognition system *"is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems."* Previous versions of facial recognition required the person to look directly at the camera, and that camera only captured a still two-dimensional photo. Modern facial recognition software utilises AI to identify people regardless of whether or not they are looking at a camera, resulting in accurate identification at angles up to 20 degrees from a full-frontal scan. Some systems can even create a three-dimensional rendering of the subject in question which can aid future identification. However, a prerequisite for successful identification are high definition cameras. On the other hand, speech recognition relates to two systems. The first system is speech processing which enables computer recognition and translation of spoken language into text, while the other is biometric identification. As defined by Markowitz (2000), voice biometrics *"uses the features of a person's voice to ascertain the speaker's identity. Systems performing this function have been applied to real-world security applications for more than a decade."*

In practice, facial recognition systems are becoming increasingly common. Biometric facial recognition in smartphones became popular when Apple launched its iPhone X in 2017. The system works by virtually projecting over 30,000 infrared dots on a person's face and analysing the pattern they form. Since then, almost all phone manufacturers followed suite and incorporated some form of facial recognition capability into their phones. Aside from smartphone identification, facial recognition systems are increasingly used in social media as well. For example, Snapchat acquired the Ukrainian company Looksery to embed their signature "Lenses" feature. Users refer to this feature as filters. Essentially, this system functions by scanning the person's face using computer vision and digitally altering facial features of users. However, the most impressive facial recognition system is the one employed by Facebook. Facebook's DeepFace system analyses pictures posted on the network and identifies specific people in the picture. This helps users automatically tag people in pictures they took. The most impressive thing about DeepFace is its accuracy. According to Brandom (2014), the system can identify a person with 97% accuracy which is even more impressive when compared to FBI's Next Generation Identification system which can identify people with an 85% accuracy. On the other hand, there are no examples of common biometric speech recognition in use today, despite the commonality of speech recognition in practice.

Similar to the private sector, public sector implementation of facial identification systems is thriving. Since 2018, the US Customs and Border Protection utilises biometric face scanners at US airports to enable speedier and more efficient boarding. Outbound passengers verify their identities by scanning their face at designated checkpoints, the system then matches the face against an identification document. Ideally, the system will replace manual checks of passports nationwide. Aside from its use in airports, some cities and countries are increasingly utilising facial recognition systems for domestic surveillance. At the forefront of these efforts is China. Most major cities in China are virtually covered end to end in AI powered facial recognition cameras. Video feed from cameras is used for a variety of purposes, most specifically the Social Credit System and Skynet. Due to a high volume of facial recognition samples, the system is becoming increasingly accurate and can be used for tracking movements of targeted individuals. As with private sector use, examples of biometric speech recognition in the public sector are lacking. An interesting example, however, is its use in the military, specifically jet fighters. Therefore, the Eurofighter Typhoon allows each pilot to create their own template used to control a wide variety of cockpit functions. Voice commands must be confirmed by visual feedback, but the system has already been proven effective in reducing pilot workload.

2.3. Digital Transformation

Previous practical implementations of digital technology pertained mostly to modifying internal operations of a company. However, researchers Ivančić et al. (2019) pointed out that the focus of implementing digital technology no longer pertains to improving internal operations, but expanding internal dimensions, reaching customers and external partners, affecting services, integrating processes, disrupting markets, and fundamentally changing industries. Therefore, in recent years, there has been a growing trend of digital transformation efforts among companies. By definition of Spremić (2017 b), digital transformation relates to the intensive and simultaneous application of digital technologies thereby creating new revenue streams and business models. A company is said to have digitally transformed if it managed to quickly and thoroughly change its core business activities such as its processes, structure and strategy. In practice, digital transformation of a company is often preceded by two distinct transformations instigated via implementing digital technologies.

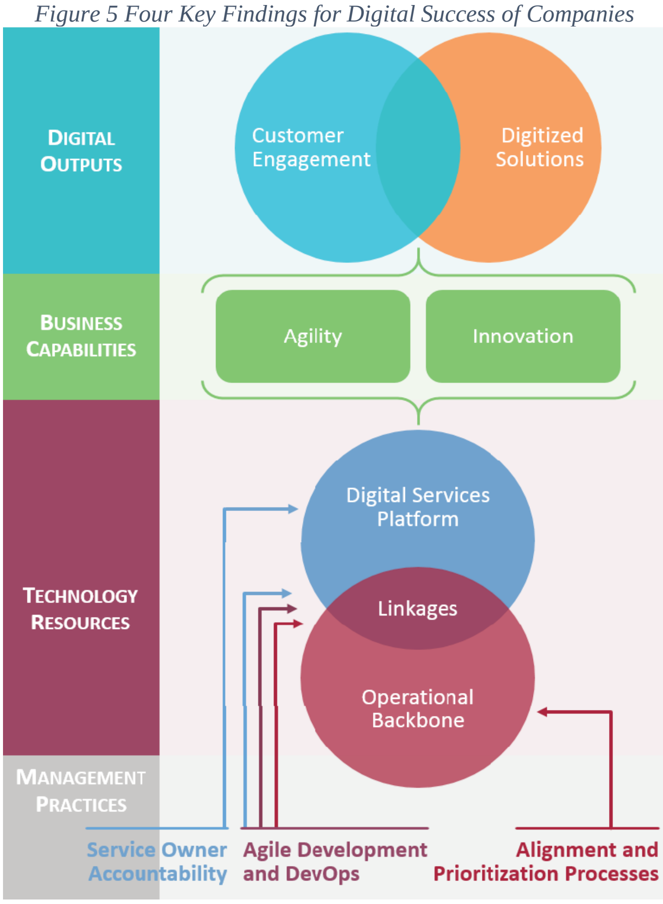
These transformations are: to become digitised and to become digital. Specifically, digitisation relies on an operational backbone, while digital relies on a digital platform. Researchers Ross et al. (2019) defined the two as: *"The operational backbone supports core operations, enhances profitability and customer satisfaction by ensuring reliable, seamless end-to-end processes through shared data and technology…The digital platform, in contrast, enables new digital offerings…To fulfil its distinct purpose, the digital platform is designed as a repository of software components that can be assembled into digital offerings that support a new or enhanced customer value proposition."* In essence, the operational backbone defines the way a company delivers goods and services, operates essential processes and keeps ledgers, while the digital platform supports digital solutions utilized by customers. Key feature of this configuration is that the operational backbone facilitates seamless operations and is mostly left unchanged, while the digital platform offers modularity and fosters quick adaptability to changes in the business environment. For example, Nike went through the process of digital transformation a while back, but changes in its business environment caused by the Covid-19 pandemic forced it to transform once more. Thanks to an established digital platform, Nike shifted its attention to engaging their customers completely digitally. Their efforts included creating digital fitness challenges where global athletes stream themselves performing a challenge which Nike's customers can perform at home. Furthermore, livestream workouts were instated every Saturday by Nike Master Trainers. These efforts brought about positive feedback from customers as well as shareholders, helping the company navigate its current hostile business environment more successfully than its rivals.

However, digital transformation efforts are not solely confined to the bounds of private companies, governmental agencies, and even entire governments, are beginning to digitally transform. For example, Australia formed the Digital Transformation Office in 2015 with a purpose of increasing transparency by digitising and publishing key documents, digitalising many public sector services and listening to public feedback. Similar efforts are present in the United Kingdom with www.gov.uk and the United States with www.usds.gov.

2.3.1. Methodology for Capturing Digital Transformation Efforts

Regarding methodology, digital transformation efforts can be captured and portrayed in many ways, however this subchapter will focus on, and outline, the methodology of Ross et al. (2017) as the same will form the basis for analysis in chapter five. Authors developed the methodology while surveying 171 senior businesses and IT leaders on digital capabilities their companies possessed. The study aimed to explore various strategies which established companies applied in order to make themselves more competitive and effective in the modern digital age. A parallel could be drawn between companies and governments as both have to rely heavily on digital technologies if they want to maximise their efficiency and provide the most benefits for their people. In the paper, authors depicted four key areas of investigation which can be seen in the figure below.

Figure 5 Four Key Findings for Digital Success of Companies



Retrieved from: https://media-publications.bcg.com/MIT-CISR-Designing-Digital-Survey.PDF (accessed 10 June 2020)

The first one concerned digital outputs of the operating model, specifically the extent to which digitised solutions were integrated into overall operations, and how personalised customer engagement was. Next, business capabilities were examined in terms of agility and innovation of the digital model. Third were the three technological resources: digital service platform, operational backbone and digital linkages in between the two. Finally, management practices served to assess service owner accountability, agility of the development process and alignment with company credo along with prioritisation processes.

Starting with the first key area, authors noted that customer engagement and digitised solutions had a sizeable impact on performance outcomes. The two are mutually reinforced and companies either develop both or none. Notable indicators of well-developed customer engagement include generating a deep insight into customers, engaging them through a personalised relationship and connecting the customers to a related community. On the other hand, indicators of settled digitised solutions comprise of enriched and meaningful information and insights, responsiveness to new environmental factors and integrating multiple services.

Moving on to digital business capabilities with agility and innovativeness, customer expectations are rapidly escalating thanks to new technologies which offer increasingly more functionality. In order to thrive in such markets, companies have to leverage their existing capabilities in order to create new offerings in an agile manner. These offerings also have to be profitable and enticing to customers in order to truly be innovative according to the authors.

The way companies become agile and innovative can be uncovered by analysing their technological environments. There are three key elements regarding the technological environment and they are: operational backbone, digital services platform and digital linkages between them. The operational backbone supports operations by providing seamless transaction processing, access to master data and unwavering security on a global scale. On the other hand, digital services comprise of the use of new technologies and leveraging partnerships to rapidly instate new functionality. Finally, digital linkages serve to connect the two in order to allow complementary functionality. Since the operational backbone and digital services are quite similar, it is noteworthy to describe prominent markings of each.

Key features of the operational backbone are:

- Automation of repetitive processes
- Access to a single source of truth
- Fostering reliable, secure and stable operations
- Modularity of functionality

Key features of digital services:

- Leverages a cloud-based platform for its operation
- Provides access to a repository of reusable business and technology services
- Leverages open source software and is API accessible
- Allows analysis of sensor data
- Allows analysis of social media data

Digital linkages allow digital services to access the operational backbone in retrieving customer master data, product master data and process transactions.

Finally, management practices are in charge of setting transformation goals and, more importantly, navigating the company through the process. The level of personal accountability of executives is closely correlated with the success of digital transformation. Next, agility in developing and implementing transformation projects is crucial for overall success. Lastly, all of the projects must be properly prioritised and aligned with overall direction of the company.

3. SOCIAL AND ETHICAL ISSUES CONNECTED TO EMPLOYING DIGITAL TECHNOLOGIES

As digital technologies evolved over time, they gradually infiltrated almost every part of our daily lives with a mission of making each day easier, more productive and enjoyable, but also drawing with them a number of social and ethical concerns. Two pressing issues regarding the implementation of digital technologies today are privacy and security. Cities around the world are increasingly covered with cameras and other surveillance devices to regulate individual behaviour in public places, while in the private sphere, mobile and social technologies enabled prompt exchange and public posting of user-generated audio, textual, photographic and video data. Most of this data is processed using AI-powered big data algorithms, allowing either private or public institutions to gather, analyse and store vast troves of data, thereby creating intricate portfolios of individual behaviours and preferences. The end result is either partial or severe obliteration of personal privacy, shifting the concern from intrusive eyes of another person to constant observation in all spheres of life. Closely related is the issue of security; over 2.7 zettabytes of data are currently stored worldwide, containing valuable personal data including identification documents, credit card numbers, records of transactions and so forth. However, as commerce shifted to its electronic alternative so did criminal activity, emphasizing the need to protect the integrity and availability of data at all times, along with thwarting unauthorized attempts at accessing data.

3.1. Privacy Concerns

An increasingly voiced issue regarding digital technology today is privacy. In the private sector, this issue is potentiated through principles of the data-driven economy. Many technological giants such as Google, Yahoo and Facebook base their business model on offering free services. Whether these services are email accounts, social media accounts, maps or even storage, all of them are gladly provided free of charge to end users. So, the question is how can these companies even survive in the marketplace, let alone thrive as they do? The answer lies in data. As detailed in the article by Anderson (2018), every user leaves a trail of personal data while browsing the web, socializing on Facebook, communicating through email or requesting directions on maps. Companies then gather, store and analyse this data in order to offer tailor-made advertisements through services which end users utilize, if some of them become enticed and click through the advert marketers pay the company in question a certain fee. This way end users enjoy free services while marketers reach their target audience more efficiently. On the downside, this equates to a loss of digital privacy. As Becker (2019) writes, the notion of privacy when people have the right to be left alone in the confines of their home is becoming null in the digital age. Furthermore, individuals are beginning to lose autonomy over their decisions because they do not yet feel as if they are observed and manipulated by targeted advertising. Big data algorithms successfully profile each individual and seduce him to participate for reasons advantageous to the company.

On the other hand, approaches to utilizing digital technologies in the public sector vary drastically from country to country. Two extremes are the European Union and China. The EU strives to safeguard personal privacy with its General Data Protection Regulation (GDPR). Strictly defining the way in which both private and public institutions can collect and use data. Conversely, China is adopting the principles of data-driven economy in its latest and largest feat of social and economic reform called the Social Credit System (SCS). Often called 'the Saudi Arabia of data', China is unparalleled in the amount of citizen-generated data as mobile payments mostly took place of hard cash and super apps like WeChat became irreplaceable pillars of daily life for almost every purpose. Yet, China is also a world leader in terms of population and pollution. The guiding thought of SCS is to make use of data citizens generated in order to combat crime and pollution, the system is based on rewarding wanted and penalizing unwanted behaviour. Aho and Duffield (2020) report that data is drawn from an intricate network of AI-powered face detection cameras placed strategically throughout major cities in the country as well as monitoring internet and social media use, analysed by machine learning algorithms. Each citizen starts off with 1,000 points, with more added or subtracted depending on his behaviour. For example, if one crosses the road during a red light, their points will immediately be subtracted, but if this person helps another and is seen doing so, their points will increase. Essentially, the system is promising to tackle most societal problems by publicly glorifying the trustworthy and vilifying wrongdoers, but it comes at the cost of personal privacy. An elaborate list of rewards and penalties can be observed in the table below.

Table 1 Table of Rewards and Penalties

Individual Rewards	*Individual Punishments*
Lower tax rates	Travel restrictions
Discounts on utilities	Blocking purchases of train/plane tickets
Deposit-free rentals	Visa restrictions
Lower interest rates	Hotel restrictions
Faster check-in at hotels and airports	Throttled internet speeds
Faster internet speeds	Restricted access to higher education
Increased access to public services	Job restrictions
Discounts on public transportation	Public shaming and blacklisting
Faster processing of travel visas	Credit restrictions
Shorter wait time at hospitals	Higher taxes and loan interest rates
Increased visibility on dating apps	Restrictions on property ownership
Firm Rewards	***Firm Punishments***
Commendations and positive publicity	Warnings
Removal of red tape and reduction of state regulation	Blacklisting mechanisms
Access to markets for public services	Market withdrawal and shutdown of e-commerce accounts
Preferential bidding on public contracts	Circulation of criticism to business partners
Granting of accreditations and qualification certifications	Public shaming/censure
Policy support	Red tape and increased administrative burdens
Administrative approvals	Unfavourable loan conditions
Tax incentives	Higher taxes than compliant competitors
Access to preferential credit services	Restrictions on stock or bond investments
Access to investment opportunities	Decreased opportunity to participate in publicly funded projects
Open markets and unrestricted foreign investment opportunities	Mandatory government approval for investments, even in sectors where market access is not usually regulated
Expedited processing of permits and visas	Managers denied tickets for high-speed rail or international business flights

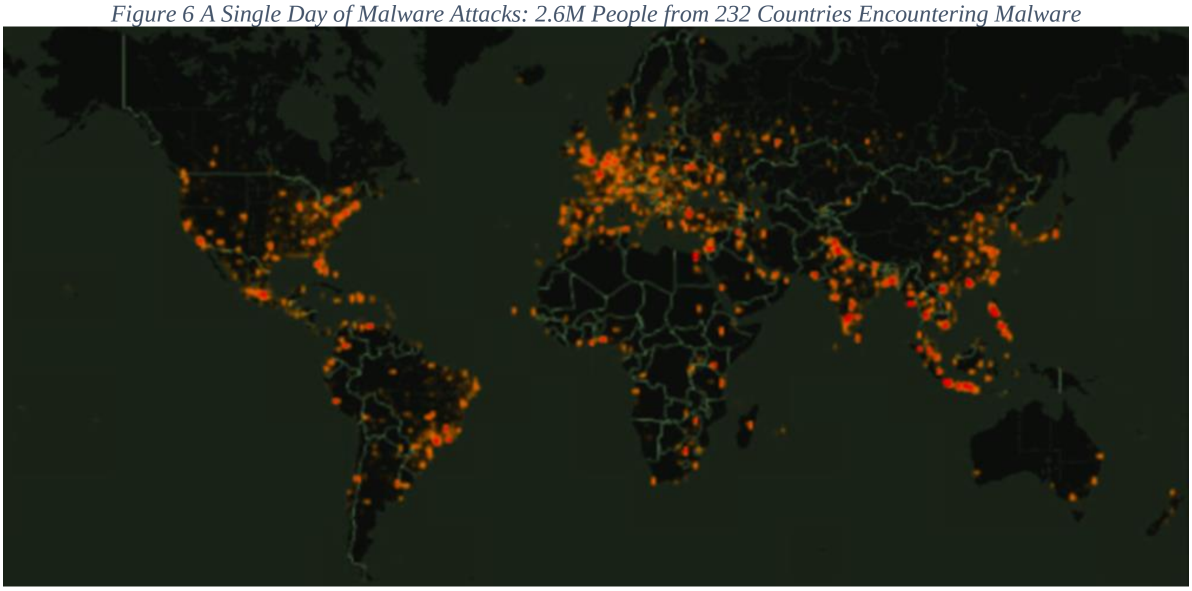
Retrieved from: Aho, B., & Duffield, R. (2020) (accessed 15 June 2020)

Another cause for concern is that SCS shares the platform with Skynet, China's elaborate AI powered police surveillance system. An iteration of this system is utilized in China's western province of Xinjiang to coerce, induce and ethnically sort the Uyghur Muslim minority under the claim of public safety. Author Leibold (2019) depicts these actions in his work on the subject, stating that Uyghur Muslims are being oppressed by way of broad and constant surveillance, therefore eroding the chance to lead a normal life. This poses the question whether the end result of reducing criminal activity can justify the means of personal privacy is obliteration.

3.2. Security Challenges

Aside from privacy issues, this encompassing reliance on digital infrastructure and services present in both private and public sector institutions brings with it the problem of security. Attempts of malicious attacks aimed at paralysing services or stealing data occur multiple times a day. One such example from the private domain is the Yahoo breach of 2014 when Russian hackers managed to steal data from 3 billion accounts including people's names, phone numbers, password recovery emails and a cryptographic value of each account via a spearphishing email. Another comes from Facebook where more than 540 million records about its users were publicly hosted on Amazon’s cloud. Data included account names, IDs, list of friends, photos and even location check-ins. Aside from companies, hackers are also targeting individuals, Microsoft reports that during a recent typical day, 2.6 million people were targeted by a newly discovered malware across 232 countries. The attacks included 1.7 million distinct, never before seen malware and 60% of attacks were over within an hour.

Figure 6 A Single Day of Malware Attacks: 2.6M People from 232 Countries Encountering Malware



Retrieved from: Microsoft (2018) (accessed 18 June 2020)

New dangers are lurking in the public sector as well. The scale of possible disruption can best be observed on the example of WannaCry ransomware attack which occurred in May 2017. This global attack paralysed hundreds of IT systems including those of power plants and bank and hospital servers. Continuing digitalization of public sector services brings with it concerns about their durability. Especially because today, the possibility of infinitely more powerful cyberattacks is potentiated by artificial intelligence. AI is able to quickly and thoroughly expose flaws in the defences of a certain institution. However, as Taddeo (2019) reports, there is a bright side to utilizing AI as it can be used to monitor one’s own defences and patch all the necessary weak points. The 2016 DARPA Cyber Grand Challenge clearly depicted this possibility when seven teams challenged their AI systems to simultaneously patch their own defences and breach the other players’ lines of defence. Seeing the potential that AI has in the area of security, both defensive and offensive, it is uncertain how the future will unfold, but it is certainly an increasing cause for concern.

4. CHARACTERISTICS OF THE COVID-19 PANDEMIC

The novel coronavirus, also known as SARS-CoV-2 or 2019-nCoV was the culprit of the latest pandemic Covid-19. First cases were first identified in China near the end of 2019 in the city of Wuhan, Hubei province. According to HZJZ (2020), coronaviruses are viruses which circulate among animals and in some cases affect humans. Many animals are known to be the source of coronaviruses, most notably bats, however humans are usually infected via an intermediate carrier. For example, the intermediary for the Middle East Respiratory Syndrome coronavirus (MERS-CoV) are camels, the Severe Acute Respiratory Syndrome (SARS-CoV) coronavirus spread on humans from civet cats and for SARS-CoV-2, pangolins. After humans have been infected, they can sometimes transmit the disease to other humans. In the case of SARS-CoC-2, an ill person infects between two or three other people. Regarding the clinical spectrum of Covid-19 cases, they vary from asymptomatic forms to complete respiratory failure, multiorgan manifestations such as sepsis and septic shock and even multi-organ dysfunction. At the outset of the disease typical symptoms include a dry cough, high fever and shortness of breath, however in some cases it can be asymptomatic or include a number of other symptoms. Cascella et al. (2020) reports that most cases of infection include only a mild disease (81%), 14% are characterised as severe, while 5% are critical. The mortality rate is around 5%, although the figure was closer to around 2% at the outset, with people of advanced age and those with chronic diseases contributing to the greatest number of fatalities.

4.1. Brief History of Similar Outbreaks

Two predecessors of the novel coronavirus were SARS-CoV and MERS-CoV. Similar to Covid-19, the outbreak of SARS started in China, but in Guangdong province near the end of 2002 and was contained in mid-2003 with only four minor outbreaks detected since. Conversely, the outbreak of MERS is much more recent and active, with the first case being recorded in September of 2012, with outbreaks occurring each year since. The majority of outbreaks caused by both viruses were contained in their area of origin, China for SARS and the Arabian Peninsula for MERS. In contrast, Covid-19 has managed to spread into almost every country in the world, infecting many more people outside the domicile area as compared to inside. Symptoms of SARS and MERS infection vary, but are largely similar. Like Covid-19, most common symptoms include a dry cough, fever and shortness of breath. However, these two infections are radically different in terms of transmissibility (R0) and mortality rates. As written by Peterosillo et al. (2020), the average number of people which a carrier infects in the case of SARS is similar to Covid-19, at around three, whereas the figure is less than one for MERS. Then again, MERS is much more deadly with a mortality rate of 35%, compared to 10% in the case of SARS and 5% in the case of Covid-19. The at-risk group all three infections are people of advanced age with previously known health problems. The table below summarizes key facts about all three coronavirus outbreaks.

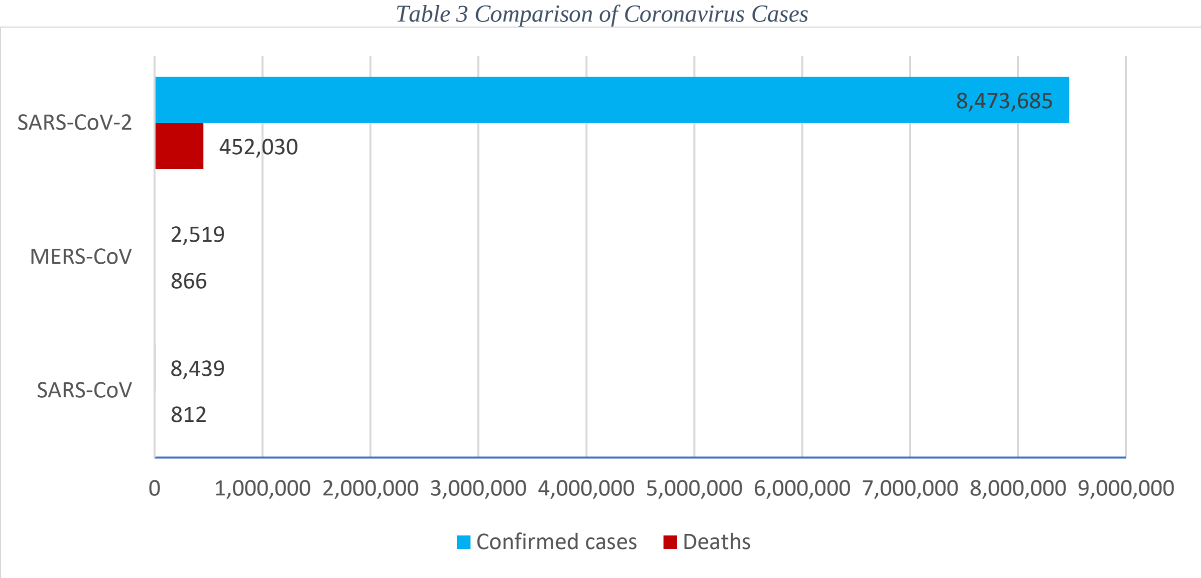
Table 2 Comparison of Major Coronavirus Strains

	SARS-CoV	**MERS-CoV**	**SARS-CoV-2**
Date and place of origin	November 2002/ Guangdong, China	June, 2012/ Jeddah, Saudi Arabia	December, 2019/ Wuhan, China
Percentage of cases contained in area of origin	63.12%	40.85%	0.98%
Confirmed cases	8,439	2,519	8,473,685
Deaths	812	866	452,030
Mortality rate	9.62%	34.38%	5.33%
R0	~3	< 1	Between 2 and 3
Initial host of transmission	Bat	Bat	Bat
Intermediate host of transmission	Palm civets	Camel	Pangolin
Affected countries	29	27	215
Age of affected individuals	1 to 91	14 to 94	< 1 to > 90

Data retrieved from: worldometers.info/coronavirus and Petrosillo, N., et al. (2020) (accessed 22 June 2020)

Nevertheless, there is one major difference between the three coronaviruses and that is the scope of outbreaks. As mentioned before, SARS and MERS were largely contained around the area of origin, reaching 29 countries in the case of SARS and 27 for MERS. In contrast, Covid-19 has quickly turned into a pandemic of global proportions, reaching over 200 countries and infecting over 8 million people at the time of writing (June 2020). The table below best portrays the scope of these outbreaks.

Table 3 Comparison of Coronavirus Cases



Data retrieved from: Martin (2020) and worldometers.info/coronavirus (accessed 22 June 2020)

4.2. Chronological evolvement into a Pandemic

First symptomatic cases of Covid-19 were first registered near the end of 2019. Scher (2020) states that the first symptomatic case occurred on November 17th, while Huang et al. (2020), argues that patient zero of SARS-CoV-2 was first documented on December 1st. In any case, the first hospital admission occurred on December 16th. Soon after, an elderly couple suffering from a fever and experiencing exacerbated coughing came seeking medical attention at the Hubei Provincial Hospital of Integrated Chinese and Western Medicine. Seeing the severity of their supposed pneumonia, the doctor decided to perform a Computed Tomography (CT) scan. Due to the abnormal nature of the results, doctor Zhang performed the same test on the couple's son and his results showed the same abnormal image. The causative agent was still unknown and such cases were classified as "pneumonia of unknown etiology", however the hospital suspected a new outbreak of infectious disease could occur so they began their own investigation. Seeing the results were indeed a cause for concern, on December 31st 2019, the Chinese Centre for Disease Control and Prevention (CDC) organized and started their own outbreak investigation program. At the same time CDC also informed the World Health Organization (WHO) about the novel, abnormal pneumonia cases. Meanwhile, municipal authorities informed the city community about an unusual pneumonia outbreak and surrounding areas already instated protective measures such as wearing protective masks, disinfecting certain public areas (Huanan Seafood Wholesale Market where the virus was thought to have originated from) and measuring temperature of travellers.

Until mid-January the virus has been spreading rapidly throughout China, but had not yet reached any other country. On the 10th of January 2020 the WHO issued a comprehensive set of guidelines to all countries with advice on how to detect, test and manage potential cases. First case outside of China was not detected until the 13th of January when Thailand confirmed its first instance. Soon after, surrounding countries, including Japan, South Korea, Taiwan, Hong Kong, Macau, Singapore and Vietnam reported cases of SARS-CoV-2 infection as well. By the end of January, active cases have been reported in 18 other countries, including Australia and European countries such as France, Spain and Italy. During the following month 37 more countries including Brazil and Croatia confirmed first instances of active cases. Meanwhile, the situation in Italy and Spain took a turn for the worse as new cases sprung up in greater frequency each day. The greatest geographic expansion of the pandemic occurred in March when 153 countries recorded first instances of active cases. During the same month, Italy overtook China in terms of cumulative deaths and near the end of March, both the USA and Spain overtook China as well. In April, cases continued to skyrocket around the world, especially in the UK and Russia. During May, things were even more hectic than before, the UK surpassed Italy in terms of active cases, but was soon overtaken by Russia. Near the end of May, Russia was exceeded by Brazil as new cases rose almost exponentially.

5. ANALYSIS OF DIGITAL TECHNOLOGIES EMPLOYED DURING THE COVID-19 PANDEMIC

5.1. Design and Methodology of Research

5.1.1. Research Objectives

The objective of this chapter is twofold, first, the aim is to depict the most protuberant and distinctive digital efforts that each of the selected countries has utilized in their fight against the Covid-19 pandemic, and second, to summarize the resulting digital transformation in tabular form. Part of the selected countries were chosen based on their importance in the global economy, such as China, the USA and Germany, while others employed certain distinct methods of curtailing the spread of Covid-19. In total, seven countries are analysed in the chapter, three from Asia: China, Taiwan and South Korea, one from North America – the USA, and three from Europe: the Germany, Croatia and Italy.

5.1.2. Research Methodology

While analysing digital solutions employed by different countries worldwide, the Digital Organization Survey conducted by Jeanne et al. (2017), proved to be an optimal methodology for encapsulating the subsequent results of each country's transformation. As described in chapter 2.3.1., authors developed the methodology while surveying 171 senior businesses and IT leaders on digital capabilities their companies possessed. The study aimed to explore various strategies which established companies applied in order to make themselves more competitive and effective in the modern digital age. A parallel could be drawn between companies and governments as both have to rely heavily on digital technologies if they want to maximise their efficiency and provide the most benefits for their people.

5.2. Overview of Digital Technologies Employed Across Asia, North America and Europe in Combating Covid-19

5.2.1. Asia

5.2.1.1. China (CN)

The epicentre of the current coronavirus outbreak was China. China was also host to the first coronavirus outbreak of SARS. Therefore, the country already had some disaster-response infrastructure from the SARS epidemic of 2002-2003. Although as Huang (2004) writes, most improvements following the outbreak were related to improving conditions in rural areas. Other improvements also included establishing a three-tiered network for disease control and prevention along with an internet-based disease reporting system which allows direct reporting of suspected cases to the Chinese CDC. Aside from its existing pandemic response infrastructure, the country also leveraged its system of digital surveillance, created in recent years, to combat the current outbreak. China was able to employ strict lockdowns and mandate digital tracking of its citizens as well as some of the most comprehensive sets of measures. Aside from contact tracing through digital tracking, China also leveraged autonomous, artificially intelligent robots in the healthcare system, AI driven drones and cameras equipped with computer vision along with its sturdy industrial internet platform in their quest to stunt the spread of Covid-19 among its population.

Contact tracing is a priority when combating the spread of Covid-19 in areas where the virus has been detected as it helps isolate potential carriers of the disease before transmission on other individuals occurs. Therefore, China mandates the use of contact tracing technology. It manages to do so thanks to its authoritarian regime and partnerships with technological superpowers based in it. Two such companies are Tencent and Alibaba. They harvest immense amounts of user data in real-time, and as such know more about population movement than the government itself. The crown jewel of Tencent's data collection efforts is its super app WeChat. It serves as a one stop shop for users who rely on it on a daily basis for conducting almost all economic activity. On the other hand, Alibaba and its Alipay platform also allow for big data collection by processing billions of transactions. It is precisely the reliance on these payment platforms that make them a perfect tool for coercing the public into complying with governmental policy. The extent of China's all-inclusive, but granular digital surveillance be observed in the case of China Electronics Technology Group (CETG). CETG is a state-owned company which created the "Close Contact Detector" application as part of the Health Check initiative powered by Alipay's Health Code system. As reported by VanderKlippe (2020), in order to travel within the province, users are mandated to sign in using QR codes scanned through their smartphones' WeChat or Alipay application along with entering their name, phone number and personal identification number. Over 200 cities in China already set up health check stations where users have to scan the code and answer a series of questions in order to determine their eligibility to travel. Once users answer all of the questions, they are given a red, amber or green QR code. Red indicates a ban on travel and requires 14-day self-isolation, it is given in cases of self-reported fever or having been diagnosed as a confirmed or suspected case of Covid-19. People who were recently in contact with a person who is classified with a red code are given an amber code and are required to self-isolate for 7 days, while others are considered healthy and safe to travel, indicated by the green QR code. Other functionality includes mapping past confirmed cases of Covid-19 positive people so users can avoid hotspots of contagion. Aside from being used for travel purposes, the health check app is used for entering the persons workplace, apartment building and various stores. Finally, user data is combined with visual input from AI powered street surveillance which covers entire cities and its transportation network. Which, when combined, means that the system is able to classify a person's state of exposure based on his proximate contact within a bus or train. However, as stated by Mehta (2020), the algorithm itself is a black box as nobody knows the extent of data which is being tracked.

China also employs visual surveillance which acts in synergy with other efforts to curb the spread of Covid-19. This is made possible thanks to an extensive infrastructure already in place, along with involvement from two prominent Chinese AI powered surveillance companies, Megvii and SenseTime. Major cities around the country are covered end to end with advanced video surveillance systems. Heaps of big data generated by those systems are analysed in real time on the cloud using deep learning algorithms. The algorithms are capturing each person's identity via facial recognition and logging their behaviour along with other relevant data into the central system. Regarding its use in the current pandemic, existing surveillance infrastructure serves to identify people who are not wearing masks in public places and penalise them accordingly. Furthermore, companies Megvii and SenseTime developed sophisticated AI-enabled thermal imaging camera systems which help determine the temperature of a person, along with the presence of protective equipment with a 99% confidence rate, using computer vision. The system is able to measure the temperature of up to 15 people simultaneously with an accuracy of $\pm0.3^{o}$C all within a single second. Such systems have been deployed around the country in places with high foot traffic such as airports, subway stations, hospitals, stores and apartment complexes among other public areas. These systems help protect people as it eliminates the need for close physical inspection of individuals while still isolating potential threats. Such AI thermal surveillance systems are increasingly being deployed among both existing and newly built hospitals to help track patients' movements within the premises. However, the government also placed these cameras in some uncommon and concerning places. In Haidian District of Beijing, high-definition cameras were placed in front of people's doors. Equipped with computer vision for human shape detection, they are capable of triggering an alarm and transmitting commands if a quarantined person attempts to leave the premises.

More concerningly, Nectar (2020) reports that in some cases cameras were even placed inside the home of the quarantined person, overlooking the door.

Aside from contact tracing and video surveillance, China is also relying on advanced robotics to combat Covid-19. An article written by Yang and Reuter (2020) outlines three ways China is using drones to fight the virus. First and foremost, drones which were originally used in agriculture for pest control were augmented to spray disinfecting chemicals on public surfaces. Next, they play a crucial role in transporting medical samples between hospitals and the CDC, making over 20 flights each day during the peak of pandemic. Finally, drones equipped with thermal cameras patrol public areas and detect individuals who are running a fever and those not wearing protective masks. On the ground, autonomous vehicles aid medical staff by delivering food and medical supplies to certain hospitals, thereby minimizing the risk of staff contagion. Another type of robot equipped with UV lamps is in charge of patrolling hospitals and disinfecting certain areas using high-power UV light. As detailed in the work of Ackerman (2020) The robot is capable of autonomous operation by scanning its surroundings using lidars and plotting the most efficient route of action. Besides alleviating the workload of the staff by autonomously performing disinfection, the robot is also markedly faster than its human counterparts with an average of two minutes per room.

The final important AI-powered technology used in combating Covid-19 again comes from the Chinese company Alibaba. The firm has developed an AI system for diagnosing patients infected with SARS-CoV-2 based on CT chest scans. The system was trained on over 5,000 CT scans of SARS-CoV-2 positive patients with an accuracy of 96%. Soon after, the system became operational and now more than 100 hospitals utilize this service. The system is becoming more and more precise as it analyses an increasing number of CT scans. Moreover, it only takes the system around 20 seconds to make its verdict, while its human colleagues need approximately 15 minutes to diagnose a patient.

5.2.1.2.Taiwan (TW)

Taiwan was the fifth country to report an active case of SARS-CoV-2 infection outside of China. Due to its proximity to China as well as a high frequency of flights between the two countries, Taiwan was expected to be the second hardest hit during the pandemic. However, that was not the case, having drawn important lessons from the 2002-2003 SARS outbreak, Taiwan had an established disaster-response system which allowed it to quickly adapt both institutionally and technologically. Thanks to this system, relevant institutions managed to integrate past 14-day travel history of each infected patient with their identification data within one day. This data was used for ongoing mobile tracking of infected individuals and was made available for clinics, hospitals and pharmacies to access. Taiwan refers to this system of mobile tracking as the 'Digital Fencing Tracking System' and it has proven to be very efficient in curtailing the spread of Covid-19 within its population. As of July 21st 2020, there have only been 446 confirmed cases and 7 deaths among its 23 million inhabitants.

Most of the measures set in place to curtail the spread of Covid-19 in Taiwan revolve around strict quarantine rules enforced by digital technologies and information sharing between relevant institutions. From the outset of the outbreak, Taiwan instated fever screenings in all of their airports, including thermal camera imaging and collecting specimens from symptomatic individuals, as well as a mandatory 14-day quarantine. Since February 14th, Taiwanese CDC also instated QR checkpoints for inbound passengers to fill out the Travelling, Occupation, Contact and Clustering (TOCC) form. Likewise, passengers travelling from highly infected areas, or those who have visited such areas in the past 14 days, were now required to enter their information into the newly developed Quarantine System for Entry. As detailed in the work of Wang and Ng (2020), Taiwan managed to integrate data from the Quarantine System for entry into its national health insurance database and share this data with clinics, hospitals and pharmacies.

Furthermore, Taiwan is among the first countries to use mobile phone location data in enforcing mandatory quarantine. Its digital fence initiative works by constantly monitoring the cellphone location and status of individuals in quarantine via cell tower information. In addition to automatic monitoring, each quarantined individual is actively monitored by local civil officers which call the individual twice a day. If the person moves away from his home, or refuses to answer the call, an alert system is immediately triggered and the individual receives more calls and messages from local authorities along with a personal visit from the local police. In case the person is found guilty of breaching his quarantine, he can be fined up to $33,000.

To aid quarantined individuals, an AI powered application called Disease Containment Expert was launched with a goal of monitoring the health status of people in quarantine. Users can interact with the app by posing health-related questions and by reporting their health status. The app also serves to inform individuals about self-health management once their quarantine ends. Another low-tech solution for supporting quarantined individuals is a governmental hotline used to arrange meal delivery, garbage collection, family visits and Covid-19 symptomatic or asymptomatic medical care services.

5.2.1.3.South Korea (KR)

South Korea was the third country to report an active case of SARS-CoV-2 infection outside of China. Similar to Taiwan, the country drew important lessons from its experience with previous outbreaks. Most notably, the MERS outbreak from 2015 which infected 186 citizens and killed 36, labelling it the largest outbreak of MERS outside the Middle East. The crux of South Korea's response was twofold. First, the country had not followed advice from the WHO regarding MERS danger zones which would imply performing and recording medical screenings of passengers travelling from such high-risk areas. Second, the country was criticised for their lack of transparency. Korean officials didn't want to disclose the names of hospitals in which the infected individuals were treated. However, both issues were properly addressed once the outbreak was contained which allowed South Korea to successfully tackle the current pandemic.

As news of the novel coronavirus outbreak reached South Korea, the country activated an emergency response system to screen all passengers aboard flights from affected areas. As with other Asian countries, this included using precise thermal cameras and isolating passengers which showed symptoms of the disease. The country also mobilised its healthcare to quickly develop and distribute tens of thousands of Covid-19 test kits to hospitals and airports among other areas. Furthermore, to curtail the spread of SARS-CoV-2 among its population, the country promptly organized drive-in testing facilities which helped detect cases of infection before they spread out of control.

Thanks to laws passed in the aftermath of MERS, the country was able to publicly disclose information about SARS-CoV-2 positive individuals on their website as well as through public alerts. As reported by Zastrow (2020), this information includes the age and sex of the infected person in addition to a detailed log of their movements. Movement information is drawn from CCTV cameras, past credit-card transactions and even smartphone GPS data. Yet, the public didn't make much use of this data as it was rather unorganized. However, this abundance of publicly available data facilitated the creation of privately developed applications which were adopted with overwhelmingly positive reviews by the public. The most popular application is called Corona 100m and it alerts users about SARS-CoV-2 positive individuals within a 100-meter radius from the user, along with their location history. The second most popular application is called Corona Map which offers similar functionality by plotting the known locations of SARS-CoV-2 positive individuals.

Eventually the Government also made its own application, but with a different goal in mind. As reported by Kim (2020), the application developed by the Ministry of the Interior and Safety serves to track health conditions and location of quarantined individuals. Named Self-Quarantine Safety Protection, the application is mandatory for suspected carriers of SARS-CoV-2 and collects GPS location data from the user's smartphone. However, due to a number of cases where individuals left their homes without smartphones, the government also issued Bluetooth wristbands for violators.

5.2.2. North America

5.2.2.1. United States of America (US)

In the past, both SARS and MERS reached the United States, but the country didn't create any notable lasting infrastructure to tackle future outbreaks. However, following the Ebola epidemic of 2014, the country put together the Global Health Security and Biodefense unit tasked with pandemic preparedness. The unit was disbanded in 2018, but part of the staff was consolidated in a new body composed of two more directorates, called the Counterproliferation and Biodefense Directorate. Still, the staff was reported to be underfunded and did not produce any valuable infrastructure for managing outbreaks. Regarding the current coronavirus outbreak, the country was fourth to report an active case of SARS-CoV-2 infection outside of China occurring during January 2020.

By the end of March, all 50 US states and territories, aside from Samoa, had documented cases of SARS-CoV-2 infection. Today (23 July 2020), the US has the highest number of confirmed cases of SARS-CoV-2 worldwide, leading its runner up (Brazil) by over one million cases. As Schneider (2020) argues in his paper on the subject, the US failed to contain the pandemic due a number of reasons. First of which is inadequate testing which was insufficiently ramped up to this day. Second, a lack of medical data sharing between the federal states, which also potentiated the problem of collecting and reporting virus testing data. Finally, instead of addressing these problems, the US chose to focus its efforts on accelerated drug and vaccine development and nonpharmacologic interventions (NPI) in terms of lockdowns.

Due to a lack of centralised initiative, technological giants in the US decided to form their own digital tracing solutions to help track the virus. The solutions come from MIT, Apple and Google. MIT led projects revolve around the PrivateKit application and a protocol called Private Automatic Contact Tracing (PACT). Both involve using anonymised and encrypted Bluetooth data from users' phones to track the number and duration of close contacts the user had with other individuals using the same service. If a user tests positive to the virus at some point in the future, the system will be able to perform a risk assessment and notify all other individuals at risk through the application. On the other hand, Apple and Google joined forces in creating their solution. Recently they launched an exposure notification API which enables interoperability between iOS and Android devices when applications from public health authorities are used. In the coming months, the companies also hope to enable a broader Bluetooth based contact tracing platform by building the functionality into underlying platforms which will be integrated in all smartphones in the world.

All of the aforementioned solutions promise to uphold strict privacy standards and are provided for the public to opt in on a voluntary basis. As mentioned before, there is no centralised initiative to utilize these solutions, but several local governments have encouraged their citizens to install the PrivateKit application.

5.2.3. Europe

5.2.3.1. Germany (DE)

In the past, Germany had not been severely impacted by either SARS or MERS, however the country managed to effectively contain the cases which eventually sprung up. In 2020, Germany was the sixteenth country to report an active case of SARS-CoV-2 infection outside of China. Contrary to the US, Germany recognized the importance of proper and timely testing so the country immediately began developing Covid-19 test kits. As a result, towards the end of January they already developed a reliable test kit which was soon rolled out for mass production. Next, although lacking in pandemic-specific infrastructure, the country was well prepared for the outbreak thanks to its digitally transformed healthcare system.

As reported in Olesch (2020), Germany started a thorough digital reinvention of its healthcare system a few years ago. Through a new legal framework and an innovation-friendly approach, many digital solutions for both patients and physicians have been implemented. First, digitization of patient records and improved communication between health centres aided transparency and improved information flow. Second, since 2018, the country has put forth great efforts in introducing telemedicine solutions which are designed to be easily integrated and require no technical know-how or hardware investments. The existence of prompt information sharing allowed healthcare institutions to distribute know-how in dealing with the virus as well as the status and number of confirmed cases. While the introduction of telemedicine solutions minimised personal contacts within healthcare institutions without sacrificing access to healthcare services.

Germany is also praised for its effective contact tracing efforts and is planning to introduce an automatic contact tracing application. The application works in much the same way as other contact tracing applications from the US. Once the application is installed, it works in the background to emit its own anonymised Bluetooth chirp and receive chirps from other users which are then stored based on proximity and duration of contact. If a user tests positive for SARS-CoV-2 sometime in the future and decides to donate his location history, the application notifies all other users with which the infected person came into prolonged contact with in order for them to get tested. Another application in development is called GeoHealth and it relies on location data which Google already stores for users of their services; its main benefit is that users can be informed about proximate contacts with much greater accuracy. Finally, a local start-up called Docyet has created an online chatbot which provides risk assessments for potentially infected individuals and also offers the option of telemedicine consultation if needed.

5.2.3.2.Croatia (HR)

Historically, Croatia didn't have any recorded instances of coronavirus infections on its territory, making it the only such country among six others analysed in this paper. Furthermore, Croatia was also an outlier when it comes to the current coronavirus outbreak with the first recorded case occurring near the end of February, much later than in other countries. Croatia initially tackled the outbreak in a timely, but restrictive manner. Relying on NPIs which included shutting down parts of the economy and mandating strict lockdowns for the majority of its citizens. Furthermore, the country performed frequent tests in its drive-in facilities to quickly isolate carriers of the disease. These measures helped to restrain the virus from propagating through society, however recently these NPIs were abolished and the country is seeking other approaches to curtailing further spread of Covid-19.

Regarding digital solutions employed in the wake of Covid-19, public sector companies are responsible for the majority of solutions. The first digital solution comes from a collaboration of the CroAI association members which resulted in the creation of a chatbot called Andrija. Andrija is an AI powered chatbot with which citizens can interact over the communication platform WhatsApp. Launched in April 2020, the service has proven to be very useful in alleviating the pressure of incoming calls from concerned citizens, thereby allowing healthcare workers to focus on more important tasks. Andrija also hosts a risk-assessment function which operates in the form of a questionnaire to determine if the person should be tested.

Furthermore, the recent abolition of NPIs potentiated the need for a contact tracing platform. Therefore, Croatia partnered up with Apis IT to create its very own contact tracing application which would record anonymized and encrypted Bluetooth connections between users based on the proximity and duration of contact. As in Germany, if an individual is confirmed positive to SARS-CoV-2, he can upload past 14-day contact data so that other users can perform tests if required. Moreover, Žabec (2020) reports that the European Commission is making efforts to unify all member state application information within a single application to more effectively track the virus inside the EU.

Finally, another Croatian company adamant to leave its mark in the fight against Covid-19 is Gideon Brothers. The company from Osijek specializes in producing AI powered robots which are capable of autonomously navigating their surroundings. Currently, the majority of their robots is used for transporting goods in warehouses, however the company is planning to equip them with high-power UV lights and disinfectant atomizers in hope to disinfect hospitals and other public areas.

5.2.3.3.Italy (IT)

The final country included in this analysis is Italy. Similar to Germany, Italy had not been severely impacted by either SARS or MERS. However, contrary to Germany, Italy has not managed to contain the outbreak in time. The country initially underestimated the potential impact of Covid-19, which is best observed in their failure to adopt already existing models of containment from China and other affected countries, opting instead for a laissez-faire approach. Coupled with inadequate testing, this resulted in a rapid increase of confirmed cases in a matter of weeks from the first confirmed case at the end of January. Once the number of cases skyrocketed, the government resorted to strict lockdown measures of the most affected areas. However, as Pisano et al. (2020) argue, this turned out to be counterproductive because many individuals fled from those infected areas into various other areas of the country hours before the mandate was passed, mostly relying on crowded public transport.

Italy is now trying to learn from its mistakes and has therefore drastically ramped up the frequency of testing. Potential carriers are now proactively traced and if they test positive, their entire family is tested and appropriately quarantined, as well as their closest neighbours. Also, special emphasis is put on home diagnosis and care as well as limiting contact with at-risk population. However, Covid-19 has exacerbated Italy's underlying data-related problems. Thanks to its regional decentralization, testing initiatives and reporting standards differ from region to region, making accurate reporting nearly impossible.

Correspondingly, owing to decentralized governing, different regions of Italy are at different stages of digital development. For example, the Trentino province in northern Italy has completely digitally transformed its healthcare system in a period of little over 10 years while other regions are still planning to do so. Trentino's TreC platform already received critical acclaim of the research community. Their integrated and evolving care model strives to empower patients and aid care providers by digitizing medical records and digitalizing patient care. From the outset of Covid-19, capabilities of the platform began to increasingly expand. TreC is now approved for telemedicine and use of chatbots along with other telemonitoring tools to help patients and protect healthcare workers. This resulted in a much more favourable epidemic picture for the province as compared with the rest of Italy.

Finally, as is the case with most countries affected by SARS-CoV-2, Italian authorities are also developing their contact tracing application. Developed at the request of the Ministry of Innovation Technology and Digital Transformation, the application called Immuni works by sending and receiving anonymous and encrypted Bluetooth pings to and from other users which is similar to other applications from Western countries.

5.2.4. Research Result Analysis

Asia has been on the forefront of historical coronavirus outbreaks. Both SARS and MERS outbreaks infected thousands and killed hundreds of people. As mentioned before, Taiwan was the most affected country outside of China during the outbreak of SARS, while South Korea suffered the strongest blow of the MERS outbreak outside the Arabian Peninsula. As a result, these and other Asian countries strengthened their infrastructure to combat future outbreaks. In addition to the pre-existing infrastructure, these three countries developed new digital solutions tailored to their needs. China had to contain further proliferation of the outbreak so it focused on creating a strong monitoring system. Taiwan was still unaffected, so strong border control and timely quarantine efforts were their primary concern. Conversely, South Korea had problems with local transmission and therefore contact tracing was their number one priority.

The response of all three countries to the outbreak of SARS-CoV-2 was prompt as all three instated checkpoints in airports, in addition to a mandatory containment period for travellers arriving from affected areas. To ensure potential carriers respected their mandated quarantine, each country developed a special system of surveillance. China relied on its well-developed system of AI powered video surveillance and expanded the number of cameras to include areas just outside people’s homes. While Taiwan and South Korea created their own mandatory applications to monitor the location and self-reported health status of quarantined individuals. However, these two applications differ in terms of the amount of personal data each collects. Taiwan’s application requires only location information from cellphone towers, while the one from South Korea mandates GPS data, and in the case of proven infection with SARS-CoV-2, a detailed history of credit card transactions.

Out of the three analysed countries, only China hosts a broader citizen monitoring platform, used for their Social Credit Scoring program. As the outbreak started, China modified the monitoring platform to alert officials if quarantined individuals are seen violating their mandated term of isolation, making participation in the system mandatory. In order to curtail community transmission, China partnered with Alipay and Tencent to instate mandatory QR checkpoints in various public places. South Korea also received help from the private sector as several developers programmed application for tracking confirmed cases of SARS-CoV-2 infection. While, Taiwan was mostly self-reliant when digital services are concerned, with the majority of private sector initiatives being tied to expedient production of protective equipment. A tabular summation of digital efforts from these three countries is shown on the page below.

Table 4 Digital Transformation of Asian Countries

ASIA			CN	TW	KR
Digital Outputs	*User Engagement*	Use of digital solutions on a voluntary basis	✗	✗	✗
		Gathering a substantial amount of personal information	✓	✗	✓
	Digitised Solutions	Prompt responsiveness to new environmental factors	✓	✓	✓
Capabilities	*Agility and Innovation*	Existence of infrastructure from past outbreaks	✓	✓	✓
		Implementation of new infrastructure	✓	✓	✓
Technology Resources	*Operational Platform*	Existence of broader citizen monitoring platform	✓	✗	✗
		Modularity of monitoring platform	✓	-	-
	Digital Services Platform	Use of at least three prominent emerging digital technologies	✓	✗	✗
		Significant use of private sector solutions in combating Covid-19	✓	✗	✓
	Digital Linkages	Allowing digital services to access the monitoring platform	✓	-	-

Contrary to Asia, the US has not developed any usable infrastructure from its experience in handling past coronavirus outbreaks. Furthermore, their poor response to the current pandemic was exacerbated by underlying inefficiencies in its healthcare system. Also, rather than leveraging the multitude of technological giants present in the country to develop a successful contact tracing platform and system of quarantine enforcement, they focused all their efforts on cure and vaccine production. Therefore, most notable digital solutions aimed at curtailing the spread of the pandemic was limited to contact tracing efforts from MIT, Apple and Google. These institutions created their own solutions which prioritize personal privacy and rely on Bluetooth connections between users who opted for using the application. This is a valiant effort which might save some lives, but for the application to be truly effective the majority of citizens should utilize the app, which seems unlikely without centralized enforcement. Lastly, a tabular summation of key digital efforts is shown below.

Table 5 Digital Transformation of the United States of America

NORTH AMERICA			US
Digital Outputs	*User Engagement*	Use of digital solutions on a voluntary basis	✔
		Gathering a substantial amount of personal information	✕
	Digitised Solutions	Prompt responsiveness to new environmental factors	✕
Capabilities	*Agility and Innovation*	Existence of infrastructure from past outbreaks	✕
		Implementation of new infrastructure	✕
Technology Resources	*Operational Platform*	Existence of broader citizen monitoring platform	✕
		Modularity of monitoring platform	-
	Digital Services Platform	Use of at least three prominent emerging digital technologies	✕
		Significant use of private sector solutions in combating Covid-19	✔
	Digital Linkages	Allowing digital services to access the monitoring platform	-

Neither of the three European countries analysed in this paper were greatly affected by previous coronavirus outbreaks, and as a result they have not developed infrastructure for containing such outbreaks in the future. However, faced with the outbreak of Covid-19, Germany and certain regions of Italy created new digital infrastructure to combat highly infectious diseases in the future. Both are focusing on continuing the digital transformation of their healthcare system in order to facilitate even faster communication and integrate telemedicine solutions which are crucial in times of crisis. The initial response to the current pandemic varied across the three countries. Germany and Croatia tackled the pandemic in a strict manner, testing and quarantining individuals very early on. Conversely, Italy opted for a more relaxed approach, choosing not to test individuals which exhibited mild symptoms of the disease. As cases of the outbreak began piling on, all three countries eventually instated lockdowns. However, some were more effective than others.

Recently, these countries decided to lift these measures in hopes of improving their economy and are resorting to digital technology for contact tracing in hopes of controlling the spread of the virus. In that effect, all three countries have decided to create their own contact tracing applications which function by sending and receiving anonymous and encrypted Bluetooth pings to and from other users. The use of this application is voluntary and if the user tests positive at some point in the future, he can choose to donate his connection history by scanning a verification code given by the testing facility. By doing so, the application is able to anonymously alert other users which the person was in prolonged close contact with. Thanks to strong data protection regulations in the EU, there are no broader citizen monitoring initiatives from any of the three analysed countries.

However, experts argue that contact tracing applications are only effective if the majority of population uses them. Since the use of these applications is voluntary and the EU boasts strong privacy protection regulations, countries cannot coerce the general public to use such services. In stark contrast, the majority of Asian countries mandate the use of contact tracing applications and services which results with greater efficiency in curtailing the spread of Covid-19. Another stark difference between the East and the West is the scope of digital technologies used in combating the virus. Eastern countries utilize a greater variety of digital technologies and they also implement them in a wider assortment of ways. Therefore, their digital transformation was much more agile and effective when faced with a novel coronavirus outbreak.

Table 6 Digital Transformation of European countries

EUROPE			DE	HR	IT
Digital Outputs	*User Engagement*	Use of digital solutions on a voluntary basis	✔	✔	✔
		Gathering a substantial amount of personal information	✕	✕	✕
	Digitised Solutions	Prompt responsiveness to new environmental factors	✔	✔	✕
Capabilities	*Agility and Innovation*	Existence of infrastructure from past outbreaks	✕	✕	✕
		Implementation of new infrastructure	✔	✕	✔
Technology Resources	*Operational Platform*	Existence of broader citizen monitoring platform	✕	✕	✕
		Modularity of monitoring platform	-	-	-
	Digital Services Platform	Use of at least three prominent emerging digital technologies	✕	✕	✕
		Significant use of private sector solutions in combating Covid-19	✔	✔	✕
	Digital Linkages	Allowing digital services to access the monitoring platform	-	-	-

6. DISCUSSION ON SOCIAL IMPACT

The implementation of digital technologies in combating the novel coronavirus pandemic has proven to be quite effective for society as a whole, however it also incited concerns about individual privacy and data security. Being on the forefront in employing both basic and emerging digital technologies in its combat against the novel virus, China elicited the most controversy, especially regarding upgrades to its existing monitoring system. The country insists on collecting immense troves of personal data from its citizens by combining surveillance camera footage, internet activity and self-reported information, but fails to explain how their algorithm actually works. These voluminous personal data collection efforts coupled with a lack of transparency evoke feelings of anxiety among the population and virtually nullify the notion of personal privacy. Moreover, actions such as the expansion of its security camera network to include areas just outside people's homes, and sometime inside as well, pose an undeniable breach of individual privacy.

Figure 7 Chinese Governments Have Been Accused of Placing Cameras Outside Homes of Quarantined Residents

Retrieved from: https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html (accessed 17 June 2020)

Authorities state that these measures are temporary, however that was also said about more encompassing mass surveillance measures during the Olympics which stayed for good. On the other hand, China has drastically increased transparency in reporting details of the novel coronavirus as compared to the SARS outbreak of 2002-2003 which helped other countries to prepare. Furthermore, its industrial internet infrastructure fostered easier communication and knowledge sharing between hospitals, thereby creating best practices for treating the virus. China also leveraged advanced digital technologies which pose less privacy and security concerns, but offer tremendous value for society. For example, the use of robots for contactless delivery as well as for disinfection purposes has helped save hours of valuable time as well as countless lives. When considered in unison, digital technologies helped China to combat the outbreak much more efficiently than it otherwise could, however, some of its actions pose an immediate threat to personal discretion and security.

The scope of digital technologies employed by South Korea is narrower than in China and the methods for contact tracing differ. As a result of poor transparency during the MERS outbreak, the government of South Korea promised to base its current response on openness and transparency. In 2016, the country passed laws which allowed collection and publication of citizen data for combating outbreaks. This meant that if an individual tests positive for SARS-CoV-2, authorities can and will use CCTV footage, credit card transaction history and smartphone GPS data to plot the person's location history, publicly uploading it along with their age and sex on their website. Although data is posted anonymously, this method of contact tracing relies on encompassing and intimate details which could give away defining details of the infected person. This could also lead to proliferation of social stigma surrounding the people infected with the virus. Another point of concern is the use of precise GPS data for enforcing mandatory quarantines. All quarantined individuals are required to download the tracking application and enable GPS surveillance, violators who disable the application from tracking them are given Bluetooth wristbands which they have to wear until their quarantine ends. This approach to containing the virus seems a bit excessive when other equally effective solutions are considered.

In stark contrast to both countries, Taiwan has been praised for its responsible use of big data. Although encroaching on personal privacy, the country does so in an accountable manner. Instead of utilizing precise GPS data for locating individuals in quarantine, the country opted for using cellphone tower information coupled with human labour in performing validation calls twice a day. This way the precise location of individuals is unknown, while still allowing local authorities to take action if the individual strays too far from home. Furthermore, Taiwan leveraged digital technologies for successfully identifying and isolating initial carriers of the virus, thereby eliminating the need for intrusive tracing measures. The country also aimed to ease the effect of quarantine-induced stress on individuals by issuing care packages and organizing an array of services aiding speedy recovery.

In general, Asian countries tend to be collectivistic societies and are therefore willing to furlough some privacy for greater public good. This can also explain the lack of strict privacy protection legislatives. However, countries from the Western world tend to have a higher threshold when it comes to upkeeping personal privacy. None more so than the US whose citizens fought against government oversight for a number of years. That is part of the reason why sudden mandatory lockdowns in the US resulted in mass protests. The country failed to convey the danger SARS-CoV-2 poses to human health early on and then responded with stern measures once the virus proliferated among the population. Consequence of this was even greater spread of Covid-19 throughout the US which had a devastating effect on society, resulting in the most drastic increase of confirmed cases anywhere in the world. Next, voluntary involvement of Apple and Google in creating a contact tracing platform is laudable, but not without problems. It is perhaps the greatest example of the trade-off between personal privacy and greater public good. When using the contact tracing platform, an individual is voluntarily permitting the two companies to collect and analyse data linked to his account, which may be used for purposes other than solely contact tracing. This means that he is helping to protect his health and the health of others who use the same service, but at the same time he is losing a part of his personal privacy.

Essentially, this is one of the most pressing question with which citizens across the world will soon be faced with, as the existence of strong privacy protecting regulation prohibit governments from mandating contact tracing technologies and most NPIs have been abolished or weakened. Instead, the use of such applications is left to individuals to decide for themselves which helps protect personal privacy, but threatens the greater good as inadequate and sparse use of such services has a negligible effect on curtailing the spread of Covid-19. However, European countries demonstrated the importance of having a strong, digitally transformed healthcare system in fighting outbreaks. The use of telemedicine and digital patient records has a sizeable positive social impact while still protecting one’s privacy.

7. CONCLUSION AND DIRECTIONS FOR FUTURE WORK

7.1. Final Remarks

From analysing the responses of different countries to the novel coronavirus, one thing is blatantly clear. Proper and timely implementation of digital technologies can have a dramatically positive effect in containing and treating infectious outbreaks. However, it is also critical to protect personal privacy and security when designing containment measures. Owing to communications technologies and platforms which are ubiquitously available throughout most of the world, there is already an abundance of data regarding different approaches to containing Covid-19 and their efficacy so far. This allows governments to adapt more swiftly by adopting best practices utilized in other countries. Out of the seven countries analysed in this paper, Taiwan hosts the best combination of digitally enforced measures which helped drastically contain the spread of Covid-19, while encroaching as little as possible on personal privacy. Unquestionably, European solutions fair better in terms of personal privacy and are on a voluntary basis, however the issue with voluntary adoption of digital technologies is their inefficiency when sparsely adopted by the public.

7.2. Limitations

The main limitation of this paper is the relative novelty of the current Covid-19 pandemic, combined with a limited timeframe of research. This paper was written in the period from the end of March until the beginning of July 2020, during which the pandemic evolved, and is still evolving, in very unpredictable ways. Due to this, some of the measures employed by the abovementioned countries may prove to be counterproductive as time goes by.

7.3. Suggestions for Further Research

From today's standpoint it is hard to imagine how long the SARS-CoV-2 outbreak will last and how effective current measures for its containment and tracking will be in the future as most countries are already witnessing the second wave of Covid-19. Since most countries instated some form of lockdowns during the initial wave of the pandemic, their economy weakened and resulted in less stringent NPIs at the beginning of the second wave. Therefore, in further research, it would be interesting to compare how countries reacted to the second wave as opposed to the initial outbreak.

LIST OF REFERENCES

Abu-Shanab, E. and Estatiya, F. (2017). 'Utilizing Cloud Computing in public sector cases from the world.' *2017 International Conference on Applied System Innovation (ICASI)*. [online] Available at: doi: 10.1109/icasi.2017.7988265 (Accessed: 16 April 2020).

Ackerman, E. (2020). *Autonomous Robots Are Helping Kill Coronavirus in Hospitals.* IEEE. [online] Available at: https://spectrum.ieee.org/automaton/robotics/medical-robots/autonomous-robots-are-helping-kill-coronavirus-in-hospitals (Accessed 23 June 2020).

Aho, B. and Duffield, R. (2020). 'Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China.' *Economy and Society*. (pp. 1–26). [online] Available at: doi:10.1080/03085147.2019.1690275 (Accessed 15 June 2020).

Anderson, C. (2018). *Free! Why $0.00 Is the Future of Business.* [online] Available at: https://www.wired.com/2008/02/ff-free/?currentPage=all (Accessed 15 June 2020).

Arsenijevic, U. and Jovic, M. (2019). 'Artificial Intelligence Marketing: Chatbots.' *2019 International Conference on Artificial Intelligence: Applications and Innovations (IC-AIAI).* [online] Available at: doi:10.1109/ic-aiai48757.2019.00010 (Accessed 23 May 2020).

Becker, M. (2019). 'Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy.' *Ethics and Information Technology 21*. (pp. 307–317). [online] Available at: https://doi.org/10.1007/s10676-019-09508-z (Accessed 15 June 2020).

Bostrom, N. (2006). 'How long before superintelligence?' *Linguistic and Philosophical Investigations, 5(1).* (pp. 11-13). [online] Available at: https://www.nickbostrom.com/superintelligence.html (Accessed 17 May 2020).

Brandom, R. (2014). *Why Facebook is beating the FBI at facial recognition.* [online] Available at: https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition (Accessed 30 May 2020).

Cascella, M., Rajnik, M., Cuomo, A., Dublebohn, S. C. and Di Napoli, R. (2020). *Features, Evaluation and Treatment Coronavirus (COVID-19).* Updated 2020 May 18. Treasure Island, FL: StatPearls Publishing. [online] Available at: https://www.ncbi.nlm.nih.gov/books/NBK554776/ (Accessed 21 June 2020).

Clement, J. (2020) *Global Digital Population 2020.* Statista. [online] Available at: www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed: 7 April 2020).

Copeland, B. (2020). *Artificial intelligence.* Encyclopedia Britannica. [online] Available at: https://www.britannica.com/technology/artificial-intelligence (Accessed 17 May 2020).

European Parliament. (2014). *Mapping Smart Cities in the EU. Study. Policy Department A: Economic and Scientific Policy*. [online] Available at:

https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.pdf (Accessed 30 April 2020).

Gao, W., Emaminejad, S., Nyein, H., Challa, S., Chen, K., Peck, A., Fahad, H., Ota, H., Shiraki, H., Kiriya, D., Lien, D., Brooks, G., Davis, R. and Javey, A. (2016). 'Fully integrated wearable sensor arrays for multiplexed in situ perspiration analysis.' *Nature, 529 (7587).* (pp. 509-514). [online] Available at: doi:10.1038/nature16521 (Accessed 7 May 2020).

Gartner (2020). *Gartner Says Global Smartphone Sales Fell Slightly in the Fourth Quarter of 2019*. [online] Available at: https://www.gartner.com/en/newsroom/press-releases/2020-03-03-gartner-says-global-smartphone-sales-fell-slightly-in (Accessed: 3 April 2020).

Gartner. (no date a). *Gartner Glossary – Smartphone.* [online] Available at: https://www.gartner.com/en/information-technology/glossary/smartphone (Accessed: 3 April 2020).

Gartner. (no date b). *Gartner Glossary – Big Data.* [online] Available at: https://www.gartner.com/en/information-technology/glossary/big-data (Accessed: 18 April 2020).

Graziani, T. (2019). *What are WeChat Mini-Programs? A Simple Introduction.* [online] Available at: https://walkthechat.com/wechat-mini-programs-simple-introduction/ (Accessed: 4 April 2020).

Guizzo, E. (2018 a). *What Is a Robot?* IEEE. [online] Available at: https://robots.ieee.org/learn/what-is-a-robot/ (Accessed 11 May 2020).

Guizzo, E. (2018 b). *Types of Robots.* IEEE. [online] Available at: https://robots.ieee.org/learn/types-of-robots/ (Accessed 11 May 2020).

Huang Y. (2004). 'The Sars Epidemic And Its Aftermath In China: A Political Perspective'. *Learning from SARS: Preparing for the Next Disease Outbreak: Workshop Summary.* Washington, DC: National Academies Press [online] Available at: https://www.ncbi.nlm.nih.gov/books/NBK92479/ (Accessed 22 June 2020).

Huang, C., Wang, Y., Li, X., Ren, L., Zhao, J., Hu, Y., Zhang, L., Fan, G., Xu, J., Gu, X., Cheng, Z., Yu, T., Xia, J., Wei, Y., Wu, W., Xie, X., Yin, W., Li, H., Liu, M., Xiao, Y., … Cao, B. (2020). 'Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China.' *Lancet (London, England), 395(10223).* (pp. 497–506). [online] Available at: https://doi.org/10.1016/S0140-6736(20)30183-5 (Accessed 22 June 2020).

Hussein, A. (2015). 'Wearable computing: Challenges of implementation and its future.' *2015 12th Learning and Technology Conference*. [online] Available at: doi:10.1109/lt.2015.7587224 (Accessed 7 May 2020).

HZJZ. (2020). *Questions and answers on novel Coronavirus (2019-nCoV).* [online] Available at: https://www.hzjz.hr/sluzba-epidemiologija-zarazne-bolesti/questions-and-answers-on-novel-coronavirus-2019-ncov/ (Accessed 21 June 2020).

Ivančić, L., Vukšić, V., Bosilj, V. and Spremić, M. (2019): 'Mastering the Digital Transformation Process: Business Practices and Lessons Learned.' *Technology Innovation Management Review, 9(2).* (pp. 36-50). [online] Available at: http://doi.org/10.22215/timreview/1217 (Accessed 3 June 2020).

Kharpal, A. (2019). *Everything you need to know about WeChat - China's billion-user messaging app.* CNBC. [online] Available at: https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html (Accessed: 4 April 2020).

Kim, Gang-Hoon and Chung, Ji-Hyong. (2014). 'Big Data Applications in the Government Sector: A Comparative Analysis among Leading Countries.' *Communications of the ACM. 57.* (pp. 78-85). [online] Available at: doi:10.1145/2500873 (Accessed 18 April 2020).

Kim, M. (2020). *South Korea is watching quarantined citizens with a smartphone app.* MIT Technology Review. [online] Available at: https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/ (Accessed 24 June 2020).

Kumar, H., Singh, M., Gupta, M. and Madaan, J. (2020). 'Moving towards smart cities: Solutions that lead to the Smart City Transformation Framework.' *Technological Forecasting and Social Change, 153*. [online] Available at: doi:10.1016/j.techfore.2018.04.024 (Accessed 30 April 2020).

LAI, L. (2010). 'Social Commerce – E-Commerce in Social Media Context'. *International Journal of Economics and Management Engineering, 4(12).* (pp. 2213 – 2218). [online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.865.9668&rep=rep1&type=pdf (Accessed: 7 April 2020).

Leibold, J. (2019). 'Surveillance in China's Xinjiang Region: Ethnic Sorting, Coercion, and Inducement.' *Journal of Contemporary China.* (pp. 1–15). [online] Available at: doi:10.1080/10670564.2019.1621529 (Accessed 17 June 2020).

Mahajan, A., Pottie, G. and Kaiser, W. (2020). 'Transformation in Healthcare by Wearable Devices for Diagnostics and Guidance of Treatment.' *ACM Transactions on Computing for Healthcare, 1(1).* (pp. 1-12). [online] Available at: doi:10.1145/3361561 (Accessed 7 May 2020).

Mander, J. (2019). *Global Web Index Flagship Report 2019.* [online] Available at: www.globalwebindex.com/ (Accessed: 7 April 2020).

Marinescu, D. C. (2018). 'Cloud Service Providers and the Cloud Ecosystem.' *Cloud computing: theory and practice*. Cambridge, MA: Elsevier. (pp. 13–22).

Markowitz, J. A. (2000). 'Voice biometrics.' *Communications of the ACM, 43(9).* (pp. 66-73). [online] Available at: doi: 10.1145/348941.348995 (Accessed 30 May 2020).

McAfee, A. and Brynjolfsson, E. (2014). Big Data: The Management Revolution. Harvard Business Review. [online] Available at: https://hbr.org/2012/10/big-data-the-management-revolution (Accessed 18 April 2020).

Mehta, I. (2020). *China's Coronavirus Detection App Is Reportedly Sharing Citizen Data with Police.* The Next Web. [online] Available at: https://thenextweb.com/china/2020/03/03/chinas-covid-19-app-reportedly-color-codes-people-and-shares-data-with-cops/ (Accessed 23 June 2020).

Microsoft. (2018). *Protecting the protector: Hardening machine learning defenses against adversarial attacks.* [online] Available at: https://www.microsoft.com/security/blog/2018/08/09/protecting-the-protector-hardening-machine-learning-defenses-against-adversarial-attacks/ (Accessed 18 June 2020).

Nectar, G. (2020) *China Is Installing Surveillance Cameras Outside People's Front Doors ... and Sometimes inside Their Homes.* CNN. [online] Available at: https://edition.cnn.com/2020/04/27/asia/cctv-cameras-china-hnk-intl/index.html (Accessed 23 June 2020).

Niku, S. B. (2011). ‘Fundamentals.’ *Introduction to robotics: Analysis, control, applications.* Second edition. Hoboken, NJ: Wiley. (pp. 1-5).

NIST. (2011). *The NIST definition of cloud computing.* NIST Special Publication [online] Available at: http://csrc.nist.gov/publications/PubsSPs.html#800-145 (Accessed: 15 April 2020).

O'Dea, S. (2020). *Smartphone users worldwide 2020*. Statista. [online] Available at: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (Accessed: 3 April 2020).

OECD/ITU. (2011). ‘M-Government: Mobile Technologies for Responsive Governments and Connected Societies’ *OECD Publishing*. [online] Available at: https://doi.org/10.1787/9789264118706-en (Accessed: 5 April 2020).

OECD/ITU. (2014). ‘Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers.’ *OECD Publishing.* (pp. 13-44). [online] Available at: doi.org/10.1787/5jxrcmghmk0s-en (Accessed: 7 April 2020).

Olesch, A. (2020) *Germany benefits from digital health infrastructure during COVID-19 pandemic.* [online] Available at: https://www.healthcareitnews.com/news/europe/germany-benefits-digital-health-infrastructure-during-covid-19-pandemic (Accessed 26 June 2020).

Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). ‘Algorithmic risk assessment policing models: lessons from the Durham HART model and “Experimental” proportionality.’ *Information & Communications Technology Law, 27(2).* (pp. 223–250). [online] Available at: doi:10.1080/13600834.2018.1458455 (Accessed 27 May 2020).

Panetta, K. (2019). *Gartner Top 10 Strategic Technology Trends for 2020.* Gartner. [online] Available at: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/ (Accessed 11 May 2020).

Petrosillo, N., Viceconte, G., Ergonul, O., Ippolito, G. and Petersen, E. (2020). 'COVID-19, SARS and MERS: are they closely related?' *Clinical Microbiology and Infection, 26(6).* (pp. 729-734). [online] Available at: doi: 10.1016/j.cmi.2020.03.026 (Accessed 22 June 2020).

Pike, J. (no date). *HSU001 unmanned submarine.* [online] Available at: https://www.globalsecurity.org/military/world/china/hsu001.htm (Accessed 13 May 2020).

Pisano, G., Sadun, R. and Zanini, M. (2020). *Lessons From Italy's Response To Coronavirus.* Harvard Business Review. [online] Available at: https://hbr.org/2020/03/lessons-from-italys-response-to-coronavirus (Accessed 28 June 2020).

Ross, J. W., Sebastian, I. M., Beath, C. M. and Jha, L. (2017). 'Designing Digital Organizations—Summary of Survey Findings.' *MIT Sloan CISR Working Paper No. 415.* [online] Available at: https://media-publications.bcg.com/MIT-CISR-Designing-Digital-Survey.PDF (Accessed 10 June 2020).

Ross, J., Beath, C., and Mocker, M. (2019). *Digital Success Requires Breaking Rules.* [online] Available at: https://cisr.mit.edu/publication/2019_1001_BreakingRules_RossBeathMocker (Accessed 3 June 2020).

Saha, H., Mandal, A. and Sinha, A. (2017). 'Recent trends in the Internet of Things.' *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).* [online] Available at: doi:10.1109/ccwc.2017.7868439 (Accessed 23 April 2020).

Scher, I. (2020). *The first COVID-19 case originated on November 17, according to Chinese officials searching for 'Patient Zero'.* [online] Available at: https://www.msn.com/en-us/news/world/the-first-covid-19-case-originated-on-november-17-according-to-chinese-officials-searching-for-patient-zero/ar-BB119fWJ (Accessed 22 June 2020).

Schneider, E. (2020). 'Failing the Test - The Tragic Data Gap Undermining the U.S. Pandemic Response.' *New England Journal of Medicine.* [online] Available at: doi: 10.1056/NEJMp2014836 (Accessed 25 June 2020).

Selerity SAS. (2020). *How Netflix Used Big Data And Analytics To Generate Billions*. [online] Available at: https://seleritysas.com/blog/2019/04/05/how-netflix-used-big-data-and-analytics-to-generate-billions/ (Accessed 18 April 2020).

Serokell. (2020). *Artificial Intelligence vs. Machine Learning vs. Deep Learning: What's the Difference.* Medium. [online] Available at: https://medium.com/ai-in-plain-english/artificial-intelligence-vs-machine-learning-vs-deep-learning-whats-the-difference-dccce18efe7f (Accessed 17 May 2020).

Singh, S. and Singh, N. (2015). 'Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce.' *2015 International Conference on*

Green Computing and Internet of Things (ICGCIoT). [online] Available at: doi:10.1109/icgciot.2015.7380718 (Accessed 23 April 2020).

Spremić, M. (2017 a). 'Governing Digital Technology – how Mature IT Governance can help in Digital Transformation?' *International Journal of Economics and Management Systems, 2, 1*. (pp. 214-223) [online] Available at: https://www.bib.irb.hr/934731 (Accessed: 27 March 2020).

Spremić, M. (2017). 'Što predstavlja digitalna transformacija poslovanja i zašto su nam važne digitalne poslovne platforme?' *Digitalna Transformacija Poslovanja.* Zagreb, HR: Sveučilište u Zagrebu, Ekonomski fakultet. (Pg. 38-39)

Taddeo, M. (2019). 'Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity.' *Minds and Machines, 29.* (pp. 187-191) [online] Available at: doi:10.1007/s11023-019-09504-8 (Accessed 18 June 2020).

The Straits Times. (2017). *Chinese court launches WeChat account to let litigants chat with judges on their cases.* [online] Available at: https://www.straitstimes.com/asia/east-asia/chinese-court-launches-wechat-account-to-let-litigants-chat-with-judges-on-their (Accessed: 4 April 2020).

Thorat, S.B., Nayak, S.K. and Dandale, J.P. (2010). *Facial Recognition Technology: An analysis with scope in India.* Cornell University. [online] Available at: https://arxiv.org/abs/1005.4263 (Accessed 30 May 2020).

VanderKlippe, N. (2020) *China Using High-Tech Surveillance in Battle against Spread of Coronavirus.* The Globe and Mail. [online] Available at: www.theglobeandmail.com/world/article-china-employing-high-tech-surveillance-in-battle-against-spread-of/ (Accessed 23 June 2020).

Wang, C. J., Ng, C. Y., Brook, R. H. (2020). 'Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing.' *JAMA 323(14)*. (pp. 1341–1342). [online] Available at: doi:10.1001/jama.2020.3151 (Accessed 23 June 2020).

Wang, L., Ranjan, R., Chen, J. and Bentallah B. (2013). 'Cloud Computing: An Overview.' *Cloud Computing: Methodology, Systems, and Applications.* Boca Raton, FL: CRC Press, 2013. (pp. 3–7).

Wigginton, C. (2018). *Global mobile consumer trends: Second edition*. Deloitte. [online] Available at: https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/gx-global-mobile-consumer-trends.html (Accessed: 3 April 2020).

Yang, J. and Reuter, T. (2020). *3 ways China is using drones to fight coronavirus.* [online] Available at: https://www.weforum.org/agenda/2020/03/three-ways-china-is-using-drones-to-fight-coronavirus/ (Accessed 23 June 2020).

Yeasmin, S. (2019). 'Benefits of Artificial Intelligence in Medicine.' *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS).* [online] Available at: doi:10.1109/cais.2019.8769557 (Accessed 23 May 2020).

Žabec, K. (2020) Borba protiv epidemije: 'Sustav za kontrolu zaraze bit će dostupan za nekoliko tjedana.' *Jutarnji list.* 15 May, (pp. 4-5)

Zastrow, M. (2020). *South Korea is reporting intimate details of COVID-19 cases: Has it helped?* Nature. [online] Available at: https://www.nature.com/articles/d41586-020-00740-y (Accessed 24 June 2020).

LIST OF ILLUSTRATIONS

LIST OF GRAPHS AND TABLES

CURRICULUM VITAE

europass Curriculum vitae

PERSONAL INFORMATION

Fran Škavić

10000 Zagreb

fskavic@gmail.com

https://hr.linkedin.com/in/fran-škavić-89bb65108

WORK EXPERIENCE

01/02/2018–28/02/2018

Ministry of Tourism, Zagreb (Croatia)

Voluntary intership

EDUCATION AND TRAINING

04/04/2016–27/12/2016

Soul Centered Leader

HUB 385 Academy, Zagreb (Croatia)

04/06/2017–11/09/2017

Life Coach Certification

International Association of Certified Life Coaches (IACC) (United States)

PERSONAL SKILLS

Mother tongue(s): Croatian

Foreign language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
Italian	A2	A1	A2	A2	A1
French	A2	A2	A1	A1	A2
Chinese	A1	A1	A1	A1	A1

Levels: A1 and A2: Basic user - B1 and B2: Independent user - C1 and C2: Proficient user

Common European Framework of Reference for Languages - Self-assessment grid

Communication skills

Good communication skills gained from a variety of team projects.

Advanced presentation skills grown from giving a number of presentations and polished through attendence of several Toastmasters International meetings.

Digital skills

SELF-ASSESSMENT				
Information processing	Communication	Content creation	Safety	Problem-solving
Independent user	Independent user	Independent user	Proficient user	Proficient user

Digital skills - Self-assessment grid