Approaches and Methods for Regulation of Security Risks in 5G and 6G

Hamid Jahankhani, Stefan Kendzierskyj, and Osama Hussien

Abstract The proliferation of technology is now exponential. Developments in technology, the increase in computer power and the reduction of cost, has allowed for greater accessibility, use and implementation of this technology in all sectors and industries. The evolution of smart and autonomous technologies, such as artificial intelligence and machine learning, has enabled traditionally labour intensive data analytical tasks to be conducted, quickly and efficiently. Multiple datasets and data lakes that have been siloed, are now being utilised and interconnected. Digital twin, AI, metaverse, virtual technologies are being immersed into all sectors and more importantly merged into humans where the line between reality and virtual are seeming to be the same. However, in order to succeed utilising these amazing and emerging technologies, it means that there has to be an incredible backbone and capacity to carry data; and instantaneously delivery at high speed and securely. 5G is already in its rollout and has to achieve its objectives in order for 6G to be fully onboarded and implemented in a methodical manner. The European Commission has 5G objectives and is applying funding for strategic initiatives, such as Horizon 2020. There are huge benefits for all with 5G/6G but only if they are implemented in a manner that decreases the risk they can pose to security, privacy and trust, which are core pillars that must be maintained. Smart cities will mean the data that is being collected can be analysed and in the wrong hands it poses security risks to the data/individual/nation. With such an intertwining of technologies interacting with humans and the abundance of IoT and eIoT in smart cities, there has to be a clear governance plan in place and way to manage 5G/6G to ensure success. This chapter explains the 5G/6G background, risks, benefits and highlights the need for robust governance.

Keywords 5G · 6G · Wireless · Cyberattacks · Unmanned · Smart societies · Digital twin · Metaverse · AI · Supply chain

H. Jahankhani (✉) · S. Kendzierskyj · O. Hussien
Northumbria University London, London, UK
e-mail: Hamid.jahankhani@northumbria.ac.uk

H. Jahankhani and A. El Hajjar (eds.), *Wireless Networks*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-031-33631-7_2

1 Introduction

It is imperative that with a foreseen utilisation and implementation of smart and automated systems within infrastructure and services, that consideration is taken to ensure the privacy and technology of these mechanisms and systems. Smart technologies, automated systems, and IoT are all dependant on data utilisation and with 5G/6G as the backbone of their functionality and being the carrier of the data. Securing both the communications mechanisms and the technologies themselves are key to their safe and secure implementation. It is also critical that such methodology, privacy and security frameworks are utilised to enable and instil trust in the use of these technologies, which whilst it will be critical in smart infrastructure, will also be pervasive in both nature and scope of use.

1.1 Fundamentals of Mobile Communication Technology

In 1983 almost all communications were wireless voice-centric, using analogue systems [1]. From 1983 until 2013 many generation type communications were introduced as follows:

- **First generation (1G)**: This was a mobile system and an integration of FM radios in analogue systems since manufacturing digital radio systems were expensive.
- **Second generation (2G)**: The former European GSM was transitioning from voice-centric wireless communication and changed into digital systems, such as EDGE, GPRS and GSM, where the code division multiple access (CDMA) system, was predominantly used in the USA with a bandwidth of 1.25 MHz.
- **Third generation (3G)**: From the end of 1990's, 3G was introduced into the market by connecting data and voice together.
- **3G to 4G migration**: Circa 2013, began a representative transgression from the internet at a lower data rate to the high-speed internet used for mobile videos and higher end multimedia. Both, LTE and WiMAX are part of fourth generation (4G) systems with a bandwidth of 20 MHz [1].

1.2 Technologies Behind the 5G and 6G Cellular Network

There are approximately six technologies that are collectively responsible for the existence and the function of the next generation network (NGN), the 5G cellular network. According to many specialists and researchers in this field, states that the innovative 5G is distinctive in three major features which shapes the technology to a positive extent, such as:

- Ability of multi-device connectivity
- Higher speeds

- Lower latency

More importantly the yearly subscription to mobile broadband systems showed a rapid increase in the number of individuals using it. In a 20-year global perspective, the number of devices connected to the internet demonstrate an exponential increase and by 2025 there will be around 75 billion internet-connected devices worldwide.

In order for the billions of IoT devices to interact with each other and with a base station as well as to respond to signals/requests faster and smoothly, it requires a faster and stable internet connection; which enables higher data rates for the purpose of information transfers. Therefore, 5G offers universal connectivity for machines, devices, and humans at various spectrum operating bands, because the goal is to develop a newly created network that can smoothly incorporate the fast growing number of devices into the new network [2].

5G Technology

5G is designed to be a cutting-edge technology and needed if the systems are to be smart enabled and undertake the range of emerging technologies. It is designed to allow long-distance coverage and stable connections as well as rapid data download and upload. As a result of 5G's wireless-based technology, the data migration enables a speed of 20 Gbps (Gigabyte per second) through wireless broadband connections, which simplifies the management of excessive data transmission via 5G.

However, the aspect of security and the overall intelligent connectivity system presents questions around social, technical and legal aspects. As a result, it is essential for the 5G/6G network to become a reliable and a well-developed technology, to assure safety against vicious cyberattacks and misuse of any kind.

One of the core parts of 5G networks is millimeter wave communication technology and offers wireless data transfer by settling for a higher bandwidth. However, the issue which arises from this technological concept is that the transmission distance of this particular wave is known to be limited to 100 m into the atmosphere, with regards to its deterioration, while the transmission is in progress. Ultimately, millimeter waves show a disadvantage in comparison to other wave types, which results in a fair transmission coverage.

The selection of frequency is essential in the sense that previous mobile technologies mainly used the lower frequency band. Therefore, 5G is expected to use higher frequencies within the frequency bands. However, higher frequencies decay faster than lower frequency and is comparatively more sensitive to signal losses.

If both, a lower frequency antenna and a higher frequency (HF) antenna were to transmit data at the same power/speed/data rate, the HF antenna would have a low area coverage, whereas lower frequency has not. As a result, users get higher data rates if the cell size is small. One essential part of 5G's architecture are small cells. Small cells are defined as *"low-power wireless access points that operate in licensed spectrum"* ([1], p. 64).

In order to serve high-dense urban locations with characteristic properties, such as number of users demanding high data rate capacities, small cells represent an alternative solution resulting in complementing the existing mobile network and densifying the network in crowded areas, such as hotspots (IZMF, n.d.). Also, Edfors et al. [3], support the general idea of deploying small cells to promote network densification, by overlooking numerous isolated base stations (BS) and achieve a non-homogeneous network architecture.

As a result, small cells are considered to satisfy the architectural requirements for the 5G cellular network. Ge et al. [4] state that in order for the 5G mobile network to be significantly reliant, the number of 5G base stations (BS) need to increase between 40 and 50 base stations per km^2, that is when Ge et al. ([4], p. 72) call 5G an "ultra-dense cellular network". Rodriguez [1] concluded that small cells offer an improvement in many applicative fields, such as in urban and rural areas and in applications for companies and homes, as well as an enrichment of provision in cellular capacity and coverage.

6G Technology

6G networks are the next generation of mobile communication technology, and will bring about significant improvements in terms of speed, capacity, and coverage, as well as a host of new capabilities such as immersive virtual and augmented reality experiences and ultra-reliable low-latency communication. But it also brings new challenges related to trust, security, and privacy. Trust is essential for ensuring the safety of the intertwined physical and digital worlds in 6G networks. Security is also crucial as the economy and society become more dependent on IT and networks. Privacy is a major concern as there is currently no way to determine when linked data becomes personally identifiable. These challenges are multidisciplinary, requiring solutions in technology, regulation, and ethics. Addressing these challenges are essential for the successful deployment and adoption of 6G networks [5]. Hence, a solid governance wide approach should be catered for both 5G and 6G.

The development of 6G technology also presents a number of technical challenges that need to be addressed in order to make it a reality. The following explains some of these key aspects of 6G technology:

Higher Frequency: One of the key aspects of 6G technology is the use of higher frequency bands, which have the potential to provide faster speeds and larger capacity. However, these higher frequency bands also present a number of challenges, including limited coverage and penetration, and the need for more sophisticated antenna and transmission technologies. Researchers are exploring a variety of solutions to these challenges, including the use of advanced antenna designs such as metamaterials and metasurfaces, as well as advanced modulation and multiplexing techniques [6].

Massive MIMO (multiple-input multiple-output): MIMO is expected to be used and involves the use of a large number of antennas at both the transmitter and receiver. This allows for the simultaneous transmission of multiple data streams, resulting in higher speeds and capacity. However, the implementation of massive MIMO presents a number of challenges, such as the need for high-precision calibration and the challenge of handling a large number of antennas [7]. Researchers are exploring a variety of solutions to these challenges, including the use of advanced algorithms and machine learning techniques [8].

Network slicing: Another key technology that is expected to be used in 6G is network slicing, which involves the virtual partitioning of the network into multiple independent logical networks, each with its own set of resources and characteristics. This allows for the customisation of the network for different types of applications and users, and enables the creation of new services and business models. However, the implementation of network slicing presents a number of challenges, such as the need for efficient resource allocation and the challenge of ensuring the security and isolation of different slices. Researchers are exploring a variety of solutions to these challenges, including the use of advanced optimisation techniques and blockchain technology [9].

Spatial multiplexing: Spatial multiplexing involves the use of multiple antennas at both the transmitter and receiver to transmit multiple data streams simultaneously. This allows for the increase of the data rate without increasing the transmission power, and is essential for applications such as URLLC (Ultra-Reliable Low Latency Communications). However, the implementation of spatial multiplexing presents a number of challenges, such as the need for accurate channel estimation [10] and the challenge of implementing the required signal processing algorithms [11]. Researchers are exploring a variety of solutions to these challenges, including the use of machine learning and deep learning algorithms [12].

Advanced error correction codes: Advanced error correction codes are essential for applications such as URLLC that require high reliability. These codes can significantly improve the reliability of the communication link by detecting and correcting errors that may occur during transmission. However, the implementation of advanced error correction codes presents a number of challenges, such as the need for low complexity and high decoding performance [13]. Researchers are exploring a variety of solutions to these challenges, including the use of advanced decoding algorithms and machine learning techniques.

Antenna design: This is essential for the successful implementation of technologies such as massive MIMO and spatial multiplexing. Researchers are exploring a variety of advanced antenna designs, including metamaterials and metasurfaces, which have the potential to significantly improve the performance of the communication system [6].

Wireless power transfer: Essential for a wide range of applications such as IoT, health monitoring, and wearable devices. Researchers are exploring a variety of wireless power transfer technologies, including near-field and far-field techniques, which have the potential to significantly improve the efficiency and convenience of wireless power transfer.

Overall, the goals and expectations for 6G technology are ambitious, and will require significant advances in a wide range of technical areas. However, if these goals can be achieved, 6G has the potential to revolutionise the way we communicate and interact with the world around us.

1.3 Strategic Directions from Government

The European Commission has been driving 5G technology opportunities since 2013 by establishing public–private partnerships. It was crucial, as to help seed research and accelerate innovation into 5G. To further assist the research initiatives, the European Commission committed public funding of €700 million through the Horizon 2020 Programme to support the initiatives and build an international plan for global 5G consensus.

In 2016, the Commission adopted a 5G action plan for the early deployment of 5G infrastructure across Europe with the idea being to launch 5G services in all EU Member States, by end of 2020 at the latest. Rolling further along on this plan, was to deploy a rapid uninterrupted 5G coverage in urban areas and along main transport paths, by 2025 [14].

According to the European Commission report, the EU has set its sights on additional targets to cover all populated areas with 5G by 2030 and is supporting the European 5G Observatory, so monitoring of the 5G Action Plan and Digital Decade strategy so that progress can be tracked, and reports created on preparatory actions taken by EU Member States.

Research and Innovation (R&I) initiatives on 6G technologies are now starting around the world, with the first products and infrastructures expected for the end of this decade and will transition from Gigabit to Terabit capacities and sub-millisecond response times. This will enable new applications such as real-time automation or extended reality sensing (‘Internet of Senses), collecting data for a digital twin of the physical world. In Europe, a first set of 6G projects worth €60 million was launched under the 5G-PPP. The Hexa-X flagship is developing a first 6G system concept complemented by 8 projects investigating specific technologies for 6G.

The European Commission adopted its legislative proposal for a strategic European partnership on Smart Network and Services as a Joint Undertaking in February 2021, which entered into force on 30 November 2021. The Regulation includes a public R&I investment of €900 million over the period 2021–2027. In December, the newly created Joint Undertaking on Smart Networks and Services towards 6G, adopted its first Work Programme 2021–2022 with an earmarked public funding of approximately €240 million (European Commission). The SNS JU organised its launch event “*On the Road to 6G*” at the Mobile World Congress 2022, in Barcelona on 1 March 2022. The Joint Undertaking is coordinating research activities on 6G technology under Horizon Europe as well as 5G deployment initiatives under the Connecting Europe Facility Digital and other programmes.

It is clear that without this momentum, drive and structure to rollout 5G/6G there would be great uncertainty over utilising the emerging technologies such as digital twin, virtual, AI, etc., as those technologies rely on the bandwidth and other properties that 5G/6G offers.

1.4 Smart City Impacts and Interactions with Individuals

One of the strategic purposes of the 5G/6G mobile network is its implementation within the public and service sector, as well as in multimedia. The concept of smart cities relies heavily on the success of 5G/6G and prolific use of Internet of Things (IoT), enterprise IoT and eventually Internet of Senses, which will interact with individuals with and without their knowledge.

The general categorisation of IoT can be defined by their uses and implementations as follows:

- **Connected products**—From connected consumer-level coffeemakers to connected industrial pumps, this category enables end-to-end visibility into product-centric operations. It also promises improvements or even transformation around issues like regulatory compliance and product serviceability.
- **Connected assets**—In contrast with connected products, this category involves high-value, long-lived equipment such as aircraft and industrial machinery. Connected assets link production systems with manufacturing and maintenance processes to increase asset uptime and reduce operational and repair costs.
- **Connected fleets**—This category is all about tracking, monitoring, analysing, and maintaining any assets that move—from trucks to ships to construction equipment—wherever they appear in the network. Extracting data from mobile equipment has been difficult and expensive, so the promise here is immense.
- **Connected infrastructures**—From software networks to power grids to buildings, the majority of IoT sensors are likely to end up in connected infrastructures. This category will deliver new forms of digital operational intelligence to transformation physical systems. The goals will be to drive economic growth, improve service, and allow for more effective and efficient operations and risk mitigation.
- **Connected markets**—Markets apply to any activity that involves physical space, from retail centres to farms to cities. IoT can help cities, rural areas, and other markets to optimize use of assets and natural resources; reduce energy usage, emissions, and congestion; and improve efficiency and quality of life.
- **Connected people**—This category focuses on improving work, life, and health by linking people and communities, enabling organisations to evolve into new business models, and delivering better lifestyle experiences.

Another example of smart cities and interactions with individuals is autonomous driving, which is also a core requirement that needs to operate on the 5G network. As a result, smart cities and autonomous vehicles are connected to (massive) IoT devices, which ultimately creates the Vehicle-to-Everything (V2X) communication connection. Therefore, intelligent connectivity within cities could have a massive impact on communication overall.

City planners, public sector bodies and private entities are striving to utilise smart and automated technologies and IoT in a way to not only streamline services and maximise efficiency, but to improve the level of service to the citizen/consumer and to bring an additional convenience and ease in the delivery of services. To this end, AI is being used to bring together an analysis of captured data, that traditionally has been kept in silo, dependant on the agency or reason for the collection. The compute capabilities of AI and machine learning has enabled large amounts of collected data to not only to be unified and analysed, but look for predictable patterns and behaviours. This means that smarter, more accurate, strategic and operational decisions can be made. These capabilities also mean that data can be collected and analysed in real-time, having utilised captured historic data to train the algorithmic systems. In the construct of a smart city, an example of this would be to utilise traffic sensor information from traffic lights at junctions and intersections, to monitor the flow of traffic. The patterns learned in this instance can also govern and advise on future infrastructure improvements to the road network, or when maintenance and construction is required. Coupling this data with environmental data, pedestrian information, timetables for public transportation systems provide masses of valuable data in which resources and services can be effectively and appropriately managed. The real-time data analysis of traffic flow in a city could also help emergency services navigate through the less congested streets to minimise journey times.

Data transmission and storage are key points to control within smart cities. This of course, requires the proliferation and unification not only of the stored captured data, but also the data that is collected in real-time by IoT and smart devices. It is therefore imperative that the vulnerabilities and potential threat and attack vectors of these devices is considered before their implementation into a high impact system.

Possible attacks on an IoT infrastructure could include:

- Affecting target system behaviour by directly influencing deployed sensors to provide incorrect/faulty readings
- Create sensor impostor—Obtain IoT network access credentials and create (D)DoS attack on existing sensor to inject impostor(s)
- (D)DoS attack on sensor network to disable data collection
- Intelligence—Information collection and related analysis to observe typical patterns
- Disruptions on infrastructure—make grid elements to malfunction to cause either partial of full grid failure
- Modify water processing/ventilation to go outside of safety limits
- Get access to more secure networks/cloud through IoT infrastructure
- Modification of wearable/implanted health devices to cause bodily harm

Considerations need to be taken into the exploitation of the IoT infrastructure itself, whereby unsecured devices could be infected to form a BotNet, used to attack other remote systems, and to great effect, given the number of potential susceptible hosts on an IoT network. Also, individuals' data could be seriously compromised in both a malicious and passive way. Malicious threats are clearly understood but passive collation of data is more of an unknown impact. If we think of a smart city and how much data is being collated in the background on individuals. It raises all sorts of questions on who has access to the data, if it is passed onto third parties, and so on.

1.5 Ethics and Regulations

With the official introduction of 5G in 2020, ethical aspects need a predefined review with regards to user safety and public privacy. Furthermore, regulative agreements between government, network providers and public users are needed and shape and manage the overall degree of safety and security. IEEE's [15] globally developed standards and use cases covers areas that are being monitored within 5G, for instance enabling smart cities and the Internet-of-Things, interoperability of technology as well as autonomous driving, which are connected to the internet. IEEE ([15], p. 1) also addresses potential issues, such as:

- Convergence of fixed, mobile, and broadcast services
- Multi-tenancy models
- Sustainability, scalability, security, and privacy management
- Spectrum
- Software enablement for software-defined networking (SDN), network function virtualization (NFV), mobile edge, fog computing, and virtualization.

In a report of GSMA ([16], p. 4) the term "intelligent connectivity" is what is known as the potentially rising combination of 5G, IoT, smart landscapes and Artificial Intelligence (AI). Particularly, the ethics behind the junction of 5G and AI is of interest. Seeburn [17] highlights the positive and rising features of 5G as fast, reliable and providing a proficient quality of service, which itself shifts technology through a transformation process in a sense that the handling of internet seems to be changing. On the other hand, Seeburn [17] acknowledges the importance of finding an efficient solution for enclosing AI and 5G together. Also, recognizing that AI is intended to operate systems and machines with comparative human intelligence, while being reliable and faster because systems executing tasks and analysing data are trained to eventually perform autonomously whilst acting cost-efficient. Merging speed, dependability and human-like intelligence levels, while factoring the technical aspect, rises both safety and ethical concerns [17].

However, the Internet of Things as well as AI are exposed to significant penetration attacks. Especially with the migration from current 4G/LTE-network to the 5G, the threat impact and its probability increases.

2 The Age of Digital Transformation Moving to 5G/6G

The age of digital transformation has urged the adoption of 5G/6G networks, for the demand and significant advancements in connectivity, speed, and capacity; enabling new use cases and further driving digital transformation. In the context of 5G/6G, digital leaders will also need to understand the implications and potential of these technologies, and how to leverage them to drive business value and stay competitive. Organisations can ensure that their digital transformation efforts are aligned by staying informed about the latest technological developments and trends, conducting regular technology assessments, investing in research and development, building strong partnerships with technology providers and industry experts, and encouraging a culture of innovation and experimentation within the organisation. It can also be said that the digital transformation needs to have certain key elements in order to be successful such as:

- Clear and well-defined strategies
- Strong leadership and alignment
- Effectively manage and analyse data
- Adapt to changing market conditions and consumer expectations
- Focus on continuous improvement and innovation
- Ethical and societal implications of digital transformation enabled by 5G and 6G.

The current state of digital transformation is characterised by the widespread adoption of digital technologies across various industries and the IT belief across the world [18]. This has led to a significant increase in the amount of data being generated and used, as well as the development of new business models and the automation of many processes. So, it can be said that the adoption of 5G/6G technology is expected to play a key role in driving the next phase of digital transformation by enabling new use cases and technologies, and further increasing the speed, reliability, and capacity of communications networks. The next phase of digital transformation contain several key factors (Fig. 1) that contribute to its development and realisation [19], that businesses need to achieve and enhance, while coping with the transformation procedure in order for it to be efficient as well as produce favourable results.

These requirements include adoption of new technologies such as:

- Cloud computing
- Big data analytics
- Artificial intelligence
- Quantum computing.

These technologies are driving digital transformation by enabling organisations to process and analyse large amounts of data, automate processes, and improve decision making. A key factor in the digital transformation is the current business pressures as the increasing competition and changing market conditions are driving organisations to adopt digital technologies to improve efficiency, reduce costs, and gain a

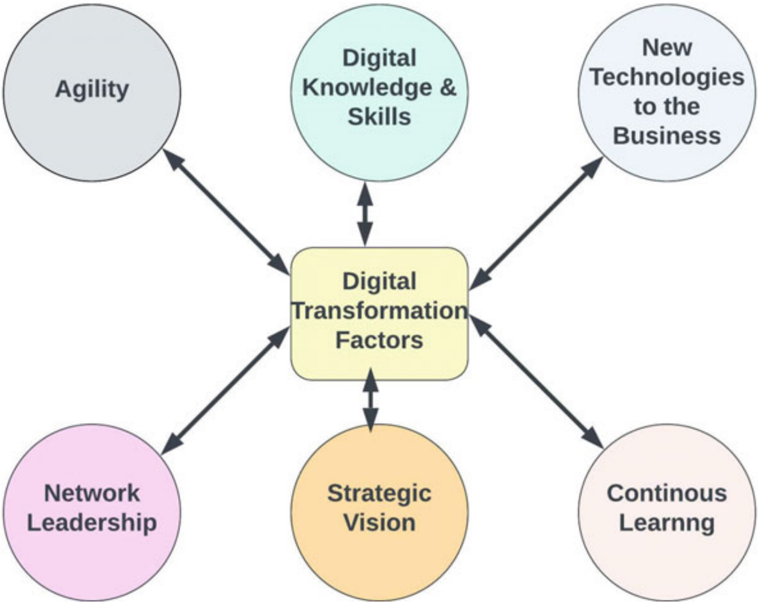

Agility
Digital Knowledge & Skills
New Technologies to the Business
Digital Transformation Factors
Network Leadership
Strategic Vision
Continous Learnng

Fig. 1 Key factors for digital transformation

competitive advantage; which in turn serves the consumer expectations for personalised, convenient, and always-on experiences. 6G networks enable organisations to support new business models and services, such as edge computing, which can help them to increase efficiency, reduce costs, and gain a competitive advantage which also enable organisations and businesses to provide faster, more reliable, and more personalised experiences for consumers. Another factor which plays a huge part in the digital transformation is the new and ongoing government regulations and policies [20]. Particularly in industries such as healthcare, finance, and energy, where there are stringent regulations around data privacy and security such as GDPR (EU, 2016).

2.1 Digital Identity and Emerging Technologies Relationship with Data Protection of Societies

Digital identity (DID), Self-sovereign identity (SSI), digital twin, blockchain and AI are all technologies that have the potential to play a significant role in protecting privacy and data in societies and below are explanations of these main technologies.

Digital identity (DID): DID refers to the unique digital representation of an individual, which is used to verify the identity of a person and grant them access to various online services. Digital identities are becoming increasingly important as more and more of our daily interactions take place online, and when combined with Self-sovereign Identity (SSI), which is an approach to digital identity that gives individuals control over their own personal data. Individuals can choose which personal information to share with others and who can access it and is seen as a way to empower individuals and give them more control over their personal data [21]. It can be used to protect privacy by ensuring that only authorised individuals have access to sensitive information (Ferdous et al. 2019).

Digital twin (DT): DT is a digital replica of a physical object or system. Digital twin can be used to model the behaviour of physical systems, such as buildings or power grids, in order to optimise their performance. In the context of privacy and data protection, digital twins can be used to analyse and protect sensitive information without exposing the actual data [22].

Blockchain technology: Blockchain is a distributed ledger system that uses cryptography to secure transactions. Blockchain can be used to create a tamper-proof record of digital transactions [23], making it useful for protecting sensitive information. Blockchain can also be used to create a secure and decentralized digital identity system [24].

Artificial intelligence (AI): AI can be used to analyse large amounts of data and identify patterns that can be used to improve privacy and data protection.

Monitoring manufacturing structure, assuring routine maintenance, and creating effective items and services are all made possible by digital twins and blockchains. They can aid in the quick and effective resolution of operational problems since they are based on dispersed network infrastructures. Nevertheless, without sufficient security, the data they contain may be susceptible to theft or misuse, possibly disclosing private company data. These technologies are anticipated to take over some occupations currently performed by people, and might have devastating impacts on some industries.

For decision-making operations, maintaining data integrity is essential, hence strict security measures are required to safeguard DTs and uphold public confidence in their usage. Although blockchains might possess the ability to improve security, there are still issues with implementation that need to be resolved [25].

AI can be used to detect and prevent data breaches, and to monitor and analyse the behaviour of individuals and systems to identify potential threats such as in SIEM and SOAR tools. AI can also be used to create personalised privacy settings and make recommendations to individuals about how to protect their personal data [26]. By giving individuals control over their own personal data, analysing and protecting sensitive information without exposing the actual data, creating tamper-proof records of digital transactions, creating a secure and decentralized digital identity system and using AI to detect and prevent data breaches, these technologies can help protect the privacy.

2.2 Current Infrastructure Weakness and Cyberattack Manipulations

When using technologies of different kinds, for instance, mobile phones, laptops, or IP-based/public networks, there is always a danger of personal data being unprotected due to a lack of proper network security and increased attack surface with the abundance of IoT devices. To add to this risk, 5G's technological specification includes the coverage of 3G and 4G/LTE. Therefore, a vast number of risk components mark critical security challenges for the 5G network.

Power supply depicts a crucial point when assessing risks, the 5G network has on users and the security structure of a nation. Ahmad [27] mentioned the tremendous criticality a collapse of wired power supply systems might have on affecting systems within the network chain, such as data handling and electrical systems, which are integrated into society and were occurred by a security breach.

With consideration of existing mobile communication networks and their specific technical protocols, for instance, HSPDA/HSPA+, GSM and LTE, individuals were gradually introduced to the power and the ability of today's technology. Telecommunication providers are eager to provide profitable services designed around maintaining customers privacy by also fulfilling information security requirements when offering Voice-IP (VoIP), national and international services, such as PABX, call and messaging services as well as roaming [28]. Therefore, the Internet of Things is exposed to a number of security threats and vulnerabilities. Ahmad et al. ([27], p. 2) point out a number of major security issues:

i. **Flash network traffic**: High number of end-user devices and new things (IoT).
ii. **Security of radio interfaces**: Radio interface encryption keys sent over insecure channels.
iii. **User plane integrity**: No cryptographic integrity protection for the user data plane.
iv. **Mandated security in the network**: Service-driven constraints on the security architecture leading to the optional use of security measures.
v. **Roaming security**: User-security parameters are not updated with roaming from one operator network to another, leading to security compromises with roaming.
vi. **Denial of Service (DoS)** attacks on the infrastructure: Visible nature of network control elements, and unencrypted control channels.
vii. **Signalling storms**: Distributed control systems requiring coordination, e.g. Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.
viii. **DoS attacks on end-user devices**: No security measures for operating systems, applications, and configuration data on user devices.

One of the most significant weaknesses of current infrastructure is the lack of proper security measures in place. Many organisations fail to implement basic security measures, such as firewalls, intrusion detection and prevention systems, and encryption. This leaves them vulnerable to attacks that exploit known vulnerabilities in their systems. For example, in 2017, the WannaCry ransomware attack affected more than 200,000 computers in 150 countries [29], exploiting a vulnerability in older versions of the Microsoft Windows operating system. This attack caused widespread disruption to businesses and organisations, highlighting the importance of keeping systems updated and patched to prevent known vulnerabilities from being exploited.

Another weakness is the use of outdated software. Many organisations continue to use older versions of software, such as operating systems and applications, that are no longer supported by their vendors. This makes it easier for hackers to exploit known vulnerabilities in these systems, as vendors typically release security updates and patches for the latest versions of their products. An example of this is the Equifax data breach in 2017 where hackers exploited a known vulnerability in an older version of the Apache Struts web application framework. This breach resulted in the personal information of over 143 million individuals being compromised [30].

The widespread use of mobile devices and cloud computing has also created new opportunities for hackers. These technologies have made it easier for hackers to gain access to sensitive information and disrupt operations. For example, a hacker could use a malware-infected mobile device to gain access to a company's network or they could use a cloud-based service to launch a distributed denial-of-service (DDoS) attack. In 2016, a DDoS attack on DNS provider Dyn used a botnet of Internet of Things (IoT) devices, such as security cameras and routers, to flood the company's servers with traffic, resulting in a widespread internet disruption.

Another example of a weakness in current infrastructure is the lack of security on the Internet of Things (IoT) devices. Many IoT devices are designed with little to no security built-in, making them easy targets for attackers. In 2018, a vulnerability in a popular IoT device, the Nest Cam, was discovered, allowing an attacker to gain access to the device's live video feed and microphone [31]. This highlights the need for manufacturers to prioritise security when designing IoT devices.

One of the main reasons why many organisations have weak infrastructure is due to a lack of investment in security and this is due to a lack of understanding of the importance of security.

The implications of weak infrastructure can be severe, including:

- Financial losses
- Damage to reputation
- Legal and regulatory penalties.

Many organisations prioritise cost-saving measures over security, and as a result, they may not allocate sufficient resources to implement and maintain robust security measures. It can lead to outdated software and hardware, which are vulnerable to known security risks and exploits. One example of this is the Target data breach in 2013, where hackers were able to gain access to the company's network by exploiting a weakness in the security of a third-party vendor. This breach resulted in the theft of 40 million credit and debit card numbers and the personal information of 70 million individuals. Target was later found to have not implemented basic security measures, such as network segmentation, and had not adequately monitored network activity [32]. This incident resulted in significant financial losses for the company and damage to its reputation.

Another example is the Sony Pictures hack in 2014, where hackers gained access to the company's network and stole a large amount of sensitive data, including personal information of employees and confidential information about upcoming films [33]. This hack resulted in significant financial losses for the company and damage to its reputation. In addition to these tangible consequences, weak security can also lead to a loss of trust from customers, partners, and other stakeholders. Organisations must take steps to address these weaknesses by implementing security measures and updating their systems to the latest versions to minimize their exposure to cyber-attacks. This includes keeping software updated and patched, implementing firewalls and intrusion detection systems, and ensuring that all devices connected to the network, including IoT devices, are secure.

New network architectures and other use cases establish fundamental concerns for 5G's security. So called "new cloud virtualization technologies such as software-defined networking (SDN) and network functions virtualization (NFV) are thought to create loopholes for vulnerabilities, which undermine the overall security of the 5G network although these network architectures excel flexibility, programmability and openness. SD × Central [34] goes further by demonstrating system downfalls due to the misuse of management interfaces of an SDN partition to attack either the overall management system or the SDN controller, which ultimately results in a security breach.

In contrary, SDN networks mainly focus on the separation of control plane from data plane by centralising control instead of standardising network protocols, whereas NFV networks focus on the replacement of certain network functions with software by using cloud computing services [35], which show a significant potential to mitigate CAPEX and OPEX, known as Capital and Operational Expenditures [27]. Lowering these expenditures show a positive benefit in the heterogeneity of 5G services, such as its functionalities and architecture because flexibility of the 5G network is, amongst other things, a key component of the divergent requirements of 5G driven applications [36].

Furthermore, the deployment of cloud services is purely based on network preferences [37]. Efficiency is an advantage feature of cloud computing because it does not own physical infrastructure for the maintenance of services, data and application ran by operators [27].

2.3 Data Privacy and Security Challenges

Data privacy and security are of paramount importance in today's digital age. With the increasing amount of personal and sensitive information being collected, stored, and shared online, organisations and individuals must take steps to protect this data from potential breaches, misuse, and lack of regulation.

One of the significant features of 5G to consider, are data handling and storing solutions. Huawei [37] points out that *'security'* as such, remains an indispensable factor for business continuity. Furthermore, Huawei [37] suggests the consideration of applying privacy and security properties from former generations of mobile network to the upcoming mobile networks, so that business continuity can be provided. By enormously mitigating the impact of security breaches and understanding the influence that risk factors have, business continuity can be subject to audit through consistent safeguarding [38].

There are essential parts of the 5G network that could lead to a higher probability of network vulnerability. Even the current network (4G/LTE) and also 5G, consist of different properties catering to different services. IoT can create exposure to numerous vulnerabilities because the technological structure exhibits potential weak spots, although it was developed based on core objectives, such as reliable network connection. Miller [39] categorically classifies "Theft", "Privacy", "Safety" as well as "Productivity" as the most significant attack types and ultimate risk factors for IoT landscapes (system, network, infrastructure). With the 5G network adding function and enhancement to the reliability and availability of faster wireless service to applications, appliances and other 5G driven technologies, the security issue gains importance and further highlight to 5G.

Although, 5G will be capable to cover high numbers of devices, machines and other appliances, the amount of data retrieved and processed will increase enormously.

That is when the confidentiality of vulnerable information may get violated and the risk for users may be immense. As Miller [39] explains, the risk of being affected of theft is especially high with the use of autonomous vehicles because hackers can get access to the vehicle's remote keyless entry system but the possibility of unauthorized access to homes are almost as high.

Huawei [37] explained that the 4G network provides an insufficient trust model because it already covers an established and bidirectional trust-relationship between *"Users"* and a *"Network",* but it does not exhibit a link between *"Users"* and the specific *"Service"* technologies (in this case the 4G mobile network) must provide (see Fig. 2).

This view is also supported by Blum et al. [40] who states that critical tasks, such as security issues arising from the verification process of computer-based systems, diminishes other arrays of problems, for instance, the reliability of a computer-based technology as well as its usability.

With the introduction of the 5G network technology into the mobile communication market there is a mutual but distinct expectation of trust on both the public and private side. Fogg and Tseng [41] state that the usability of technology is a crucial factor of trust by which a user's degree of trust is measured by. Moreover, Blum et al. [40] describe 'Trust' as an accumulation of key elements of trust, which comprise factors, such as availability, reliability and privacy, into the definition of trust with regards to the field of technology.

One of the major challenges in data privacy and security is the prevalence of data breaches. Cybercriminals are constantly devising new methods to gain unauthorised

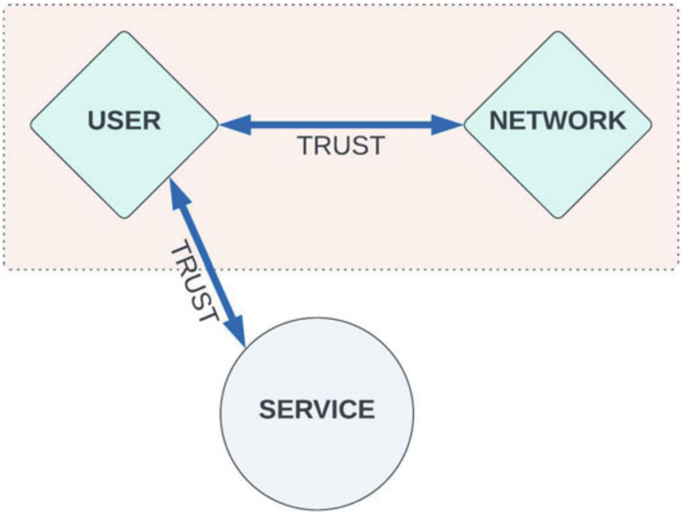


Fig. 2 Trust model of the 4G network

access to sensitive information, such as through phishing scams, malware, and other malicious techniques, according to [42]. Phishing attacks accounted for 83% of all of the attacks against business organisations and 87% for charities organisation, followed by impersonation attacks (27% and 26% respectively) and viruses and malwares (12 and 11%), and according to the same survey, there is a huge number of micro and small to medium organisation affected with data breaches in compared to large organisations, this may be the fact due to the less security measures and controls and security mentality over this organisations and businesses. These breaches can have severe consequences, including financial loss, reputational damage, and loss of trust from customers. For example, the high-profile data breaches of companies like Yahoo (NCSC, 2016) and Marriott, [42] have resulted in the compromise of millions of customers' personal information.

Another major challenge is data misuse. Even when data is not stolen, it can still be misused by companies, governments, and other organisations. This can include using personal information for targeted advertising, or sharing data with third parties without proper consent. This not only violates individuals' privacy rights but can also cause harm to the individuals in case of sensitive information. One example of this is the Cambridge Analytica scandal, in which the personal data of millions of Facebook users was harvested without their consent and used for political advertising [43]. This data can be used later for many reasons including identity thefts, which has become one of the fastest growing crimes [44]. Most people are unaware of the amount of data they disclose over the Internet. This data can be easily aggregated, data-mined and linked together.

Another challenge is the lack of regulation for data privacy and security. In many countries, there are few laws in place to protect personal data, and even where regulations do exist, they can be difficult to enforce [45]. This lack of accountability can make it easier for organisations to mishandle personal data. For example, the General Data Protection Regulation (GDPR) which was implemented in the European Union in 2018, provides strict guidelines for organisations handling EU citizens' personal data but still, there are many organisations which are not compliant with it.

Inadequate security measures are another challenge faced by organisations. Many organisations do not have the proper security measures in place to protect personal data, such as encryption or strong password policies. With the increasing use of new technologies like NFC, 5G, and the proliferation of devices, it is crucial that organisations keep their security measures up-to-date and adapt to the new challenges. For instance, with the integration of 5G networks, there will be an increase in the amount of data that can be transmitted, and the number of devices that can be connected, which will open up new attack surfaces for cybercriminals. The use of wireless networks and devices also present significant cybersecurity risks. As the number of connected devices increases, the surface area for potential security breaches expands. It is crucial that cybersecurity measures are integrated at all stages of the development and deployment of these technologies to mitigate the potential risks.

There needs to be a multifaceted approach involving both individuals and organisations. Individuals must take responsibility for protecting their personal information online by being cautious when sharing personal information online, using strong passwords, and keeping their software and devices updated. Organisations must also take necessary measures to protect personal data, including implementing robust security measures, ensuring compliance with regulations, and promoting a culture of data privacy and security.

3 Governance and Adopting Methodologies for Managing Standardisation and Interoperability

The emergence of 6G networks is set to revolutionise the way we communicate and interact with technology. With ultra-low latency and high data rate communication, 6G networks will enable new use cases and applications, such as the deployment of autonomous vehicles, intelligent transportation systems, and the internet of things at a massive scale, as well as support for advanced artificial intelligence and machine learning applications. This level of technological advancements, however, also brings new challenges, especially in terms of information governance.

Information governance (IG), as defined by the International Association for Information Governance Professionals (IAIGP), is the processes and standards that ensure the availability, integrity, and security of the data an organisation relies on to achieve its goals. It involves a wide range of issues such as security, privacy, data sharing, and regulatory compliance. As 6G networks will generate, transmit, and store a tremendous amount of data, it is crucial to have a well-defined governance framework in place to ensure the protection and safe management of this data. However, standardising IG for 6G networks poses several challenges, such as the fast-changing technology and the need for flexible standardisation approach. Additionally, there is a lack of international standards or best practices for information governance in 6G networks.

As the world becomes increasingly dependent on technology and mobile networks, the next generation of wireless communication, 6G, is being developed to address the needs of an increasingly connected society. However, the development and deployment of 6G also raises a number of governance challenges related to spectrum allocation, network security and privacy, international coordination, and the impact of emerging technologies such as artificial intelligence and the Internet of Things.

Spectrum allocation is a critical component of wireless communication and will be even more crucial for 6G networks. 6G networks will require new spectrum bands that have not been used for mobile communication before, and this will require new governance models for spectrum management. Dynamic and flexible spectrum access is also needed in 6G networks to ensure that the available spectrum is used in an efficient way.

Network security and privacy are also key considerations for 6G. With the vast amount of data generated, transmitted and stored by 6G networks, it is crucial to have robust security and privacy measures in place. 6G networks must be designed to protect sensitive information and prevent unauthorised access to the network. The governance of 6G networks must also consider the potential impact of emerging technologies such as artificial intelligence and the Internet of Things on security and privacy. International coordination is also essential for the governance of 6G. With 6G networks spanning borders, it is important to have international agreements in place to ensure that different countries' networks can interoperate. This will require cooperation between governments, the private sector, and academia.

3.1 Enabling Secure and Resilient Societies

Enabling secure and resilient societies is a critical goal for governments, organisations, and individuals around the world. The ability to protect citizens and infrastructure from natural disasters, cyberattacks, and other forms of disruption is essential for maintaining social and economic stability. In recent years, the frequency and severity of these types of incidents have increased, highlighting the need for effective and comprehensive strategies for building secure and resilient societies. One key aspect of building secure and resilient societies is the use of technology. Advanced sensors, communication systems, and analytical tools can provide early warning of potential threats and help decision-makers respond quickly and effectively.

For example, predictive analytics can be used to identify patterns of behaviour that may indicate an imminent cyberattack when coupled with artificial intelligence (AI), while advanced communication systems can enable rapid response and recovery in the event of a natural disaster. A research conducted by Masombuka et al. [46] highlight *'The Application of AI'* techniques to constantly guard the network and discuss the necessity to employ novel strategies, for instance the use of versatile, adaptive, growing, and analysis-driven AI technologies.

The worldwide industrial operations of today have more demanding needs than ever. The appropriate components for incident management choices and operations virtualisation appears to be a sensor-packed production system that ensures that every procedure or equipment component renders events and the monitoring is accessible. Also, the use of technology in building secure and resilient societies by using Internet of Things (IoT) devices. These devices can be used to monitor critical infrastructure, such as power grids, water systems, and transportation networks, and to provide early warning of potential failures or disruptions. Additionally, IoT devices can be used to track the location of emergency responders and other personnel, allowing them to coordinate their efforts more effectively. Which can be incorporated into the next industrial revolution for the cyber-physical systems [47].

Blockchain technology is another example being used to enable secure and resilient societies. It is a decentralized, distributed ledger that can be used to record transactions and other data in a way that is secure, transparent, and tamper-proof. This makes it an ideal technology for a variety of applications related to security and resilience, such as supply chain management, digital identity verification, and emergency response coordination.

Citizen engagement is another important aspect of building secure and resilient societies. This can involve educating the public about potential threats and how to prepare for them, as well as encouraging active participation in emergency management and recovery efforts. Community-based organisations, for example, can play a vital role in helping to mobilize and coordinate local response efforts [48]. Citizen science is an example of this method of scientific research. It involves the participation of citizens, who can help to collect data, report observations, and provide insights about potential hazards and vulnerabilities. Citizens can use mobile apps to report information about flood-prone areas, bushfires, or other hazards, which can help to improve the accuracy of flood and fire maps and support emergency management efforts [48].

While technology and community engagement are both important, they must be balanced with the need to maintain civil liberties and protect privacy. Governments must be transparent about the data they collect and how it is used, and they must also take steps to protect citizens from overreach and abuse of power. This can include implementing strict data protection and privacy regulations, as well as creating oversight mechanisms to ensure that these regulations are being followed.

Overall, building secure and resilient societies is a complex and ongoing process that requires the cooperation of governments, organisations, and individuals. While technology and community engagement can play a critical role, it is ultimately up to humans to manage and control these efforts to ensure that they are effective and ethical. This includes implementing effective governance, risk management, and incident response frameworks, as well as ensuring that the needs and perspectives of all stakeholders are considered. When it comes to building secure and resilient societies, there are a number of technical standards and guidelines that organisations and governments can follow to ensure that their efforts are effective and aligned with industry best practices.

One widely used standard for information security is ISO/IEC 27,001 as it provides a framework for implementing, maintaining, and continually improving an information security management system (ISMS). It covers all aspects of information security, including the management of risks, incident management, and compliance with legal and regulatory requirements. Organisations can use this standard as a guide for developing their own information security policies and procedures, and can also seek certification to demonstrate their compliance with the standard [49].

Another important standard for building secure and resilient societies is the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). This framework provides a flexible and adaptive approach for managing cybersecurity risks, and it is widely adopted by organisations in both the public and private sectors. The CSF includes a set of best practices for identifying and assessing cybersecurity risks, protecting against threats, detecting and responding to incidents, and recovering from disruptions [50] (Fig. 3).

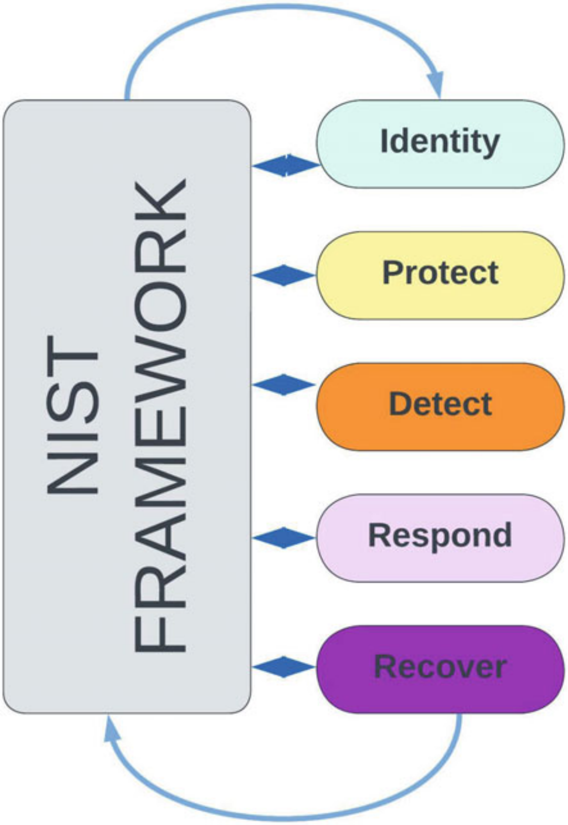
For disaster recovery and business continuity, organisations can refer to standards such as ISO 22301 and BS 25,999. These standards provide guidelines for developing and implementing effective continuity management plans, including risk assessments, incident response procedures, and recovery strategies [51, 52].

3.2 Disaster Resilience and Managing the Risks

The rise of cyber threats has become a major concern for organisations, as cyber security incidents can cause severe damage to an organisation's reputation, financial losses, and even loss of lives. Disaster resilience refers to the ability of organisations to prepare for, withstand, and recover from the impacts of disasters and security incidents. The implementation of risk management frameworks, incident response plans, and early warning systems can be effective in improving disaster resilience and reducing the impact of cyber security incidents.

It was revealed that the current state of cyber security in relation to disaster resilience is a matter of concern, as cyber threats have become more sophisticated and frequent [53]. The results from different surveys conducted revealed that many organisations are not adequately prepared to handle cyber security incidents [54]. In addition, there is a shortage of skilled individuals in the cyber security fields in Europe and due to the severe scarcity of experienced security specialists, which has been observed, the industry has been struggling to keep up with demand, which has been growing over the last few years as a result of the culture's extensive digitalisation [55].

Fig. 3 NIST Framework—key factors



It can be concluded that the risk assessment and mitigation strategies such as the use of risk management frameworks, incident response plans and early warning systems are crucial for ensuring disaster resilience, and universities should focus on ensuring that they produce more experienced individuals who are ready to take on the job market in the Cyber Security Field and fill the current shortages.

The importance of incident response plans and risk management frameworks in improving disaster resilience is emphasized by many researchers [56, 57], as well as the need for organisations to regularly test and update their incident response plans to ensure that they are effective in the event of a cyber security incident [58, 58].

The EU has made significant progress in improving its readiness against cyber threats and has established a comprehensive framework for cyber security, which includes legislation, policies, and initiatives aimed at improving the EU's cyber security posture. The EU's cyber security strategy, which was updated in 2020, sets out a clear vision for the EU's cyber security efforts and provides a framework for the EU's cyber security initiatives. The EU's cyber security agency, ENISA, plays an important role in supporting the EU's cyber security efforts, and has been instrumental in the development of the EU's cyber security framework.

4 Strengthening Trust in Complex Private and Public Supply Chains

The growing intricacy of supply chains, be it private or public, has made it challenging for organisations to gain the confidence of their customers, vendors, and other stakeholders. To overcome this challenge, companies should adopt a multifaceted approach that includes increased oversight, responsibility, transparency, robust partnerships, and a proactive approach to addressing societal issues. By implementing technologies like RFID, GPS tracking, and blockchain, companies can achieve real-time tracking of goods, evaluation of suppliers' performance and identification of potential risks. Independent verifications such as certifications and third-party audits can assure compliance with established standards, laws and regulations. Building strong relationships through regular communication and sharing of information can help identify and mitigate supply chain risks. Furthermore, addressing societal concerns such as fair labour practices, environmental sustainability and ethical business behaviour can help companies to build trust with stakeholders who are increasingly concerned about the impact of business on society.

Researchers contend that businesses may not always detect and prioritise these risks appropriately, leaving them unprepared for dangers with low likelihood but significant consequences. Trust and maintaining credibility is another factor that businesses may struggle to display. One way to tackle the issue of establishing trust in complex dependencies on public and private service providers and supply chains is through increased transparency. This can be achieved by implementing systems that provide real-time visibility into supply chain activities. For example, using technologies like RFID (Radio-Frequency Identification) tags, GPS tracking, and blockchain can help companies track the movement of goods, monitor supplier performance, and detect potential risks in their supply chains. This real-time visibility can help companies to quickly identify and respond to issues as they arise, which can help to build trust with customers, suppliers, and other stakeholders. The adoption of blockchain in supply chains is still in its early stages, as there are several technical, regulatory, and new organisational challenges that need to be overcome. These challenges include scalability, interoperability, data privacy, and regulatory compliance (looking at different geographical jurisdictions). A successful implementation of blockchain requires a collaborative approach involving all stakeholders in the supply chain, including suppliers, manufacturers, logistics providers, and customers [60].

Proactivity identifying and addressing societal issues such as labour rights, environmental sustainability, and ethical business practices is also a key aspect of building trust in the complex private and public supply chains. Companies can create and implement policies, procedures, and standards to ensure that their suppliers adhere to such societal issues. In January 2012, the California Transparency in Supply Chains Act (Senate Bill 657) (CTSCA) was enacted. The CTSCA requires that retailers and manufacturers doing business in California, with annual worldwide gross receipts of $100 million or more, must explicitly disclose their efforts to eradicate slavery and human trafficking. Companies have moved quickly to update their auditing mechanisms to ensure all supplier factories meet the requirements of the Act [61].

Cybersecurity is also a critical aspect that must be considered when strengthening trust in complex private and public supply chains, it can be said that cybersecurity in logistics and supply chain management is a growing area of concern [62]. With the increasing use of technology and digital systems in supply chain management, there is a growing risk of cyberattacks that can compromise the integrity and security of sensitive information and disrupt supply chain operations. There are many activities organisations should do to mitigate these risks and all fall into the information governance and how that is managed across all the stakeholders. Another type of model suggested is to build trust within the supply chain through a cyber security maturity model (CSMM) and combine the model with blockchain. The framework assists in an end-to-end supply chain that ensures all those that sign up to the supply chain follow the CSMM framework requirements and utilises some form of industry methodology (e.g. CMMi, ITiL, etc.) to ensure monitoring, training, compliance, etc., are adhered to on an ongoing basis. Blockchain can then be the mechanism to enhance security that allows tracking from origin all the way through the supply chain, from raw materials, manufacturing/distribution; using smart contracts, to offset criminality, counterfeiting, falsification and tampering [63].

With the importance that 5G/6G brings to both organisations and individuals it is imperative that societal and ethical impacts are taken into consideration especially as these technologies continue to advance. It will become even more crucial to ensure that they are secure, and that sensitive data is protected. Additionally, it is essential to establish transparency and trust in the decision-making processes of these systems and that they are aligned with societal issues. Organisations will need to continue to implement robust cybersecurity measures, build strong partnerships, and address societal issues in order to establish trust and ensure the success and sustainability of their operations.

5 Conclusion

Since the introduction of mobile/wireless communications, internet, devices and IoT, the need for 5G/6G adoption and its roll-out in a safe and secure manner, is becoming increasingly important. Humans are now experiencing very high levels of interaction with technology that has not been seen before and it is only set to increase and be further connected; in a way that presents more humanoid interconnected interactions. Both organisations and individuals know that data is extremely important and safeguarding it needs to have very disciplined controls and governance that has the monitoring and checks that would be expected. Whilst the use of AI, digital twin, virtual reality and other tools are there to assist and support analysing these huge data sets, they also have the capacity to allow data to fall into the wrong hands or be passed onto third parties that may make prejudgements on individuals without their knowledge. It can be further complicated with recent acceleration of satellite communications, technologies and its interaction with all other traditional systems (of which 5G/^G will be part of). What was once more military/government controlled launching of satellites into high earth orbit (HEO) is now experiencing thousands of satellites being launched by commercial companies into low earth orbit (LEO). That raises very concerning questions on how these will interact with 6G networks, and where the data will be located. If we consider what governance method is being applied here, and presents a rather large question mark on where the control, access, monitoring and security responsibilities lie.

Clearly the acceleration of emerging technologies is needed as to help support humans living now and in the future, with increasing population size and diminishing resources. We will need these 'smart' technologies and its computational power. But what is also needed is that sense of traditional discipline and governance frameworks that encompasses end-to-end the activity on 6G networks and how the data is treated and ensure it is secure, respect its privacy but not hinder the advancement of the benefits 6G will bring to all. A difficult balance to maintain, but necessary.

References

1. Rodriguez J (2015) Fundamentals of 5G mobile networks, 1st edn. Wiley, Chichester/West Sussex
2. Al-Dulaimi A, Chih-Lin I, Wang X (2018) 5G networks: fundamental requirements, enabling technologies, and operations management. 1st edn. New Jersey: Wiley
3. Edfors O, Larsson E-G, Marzetta T-L, Tufvesson F (2014) Massive MIMO for next generation wireless systems. IEEE Commun Mag, pp 186–195
4. Ge X, Mao G, Han T, Tu S, Wang C-X (2016) 5G ultra-dense cellular networks. In: IEEE wireless communications. 23(1):72–79
5. Ylianttila M et al 6g white paper: research challenges for trust, security and privacy. arXiv:2004.11665
6. Shlezinger N et al (2021) Dynamic metasurface antennas for 6G extreme massive MIMO communications. IEEE Wirel Commun 28(2):106–113
7. Rajatheva et al (2020) White paper on broadband connectivity in 6G. arXiv:2004.14247v1[eess.SP]. https://arxiv.org/abs/2004.14247
8. Chen M et al (2019) Artificial neural networks-based machine learning for wireless networks: a tutorial. IEEE Commun Surv Tutorials 21(4):3039–3071
9. Khan LU et al (2020) Network slicing: recent advances, taxonomy, requirements, and open research challenges. IEEE Access 8:36009–36028. https://doi.org/10.1109/ACCESS.2020.2975072
10. Giordani M et al (2020) Toward 6G networks: use cases and technologies. In: IEEE communications magazine 58(3):55–61. https://doi.org/10.1109/MCOM.001.1900411
11. Nayak S, Patgiri R (2020) 6G communication: envisioning the key issues and challenges. arXiv:2004.04024
12. Jagannath A, Jagannath J, Melodia T (2021) Redefining wireless communication for 6G: signal processing meets deep learning with deep unfolding. IEEE Trans Artif Intell 2(6):528–536. https://doi.org/10.1109/TAI.2021.3108129
13. Yue C et al (2022) Efficient decoders for short block length codes in 6G URLLC. arXiv:2206.09572
14. European Commission (2021) Shaping Europe's digital future: 5G. https://digital-strategy.ec.europa.eu/en/policies/5g. Accessed 19 Jan 2023

15. IEEE (2018) IEEE standards association: IEEE standards activities in 5G". Available at https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/5G.pdf. Accessed 18 Aug 2019
16. GSMA (2019) Intelligent connectivity: how the combination of 5G, AI, big data and IoT is set to change everything. Available at https://www.gsma.com/IC/wp-content/uploads/2019/02/22209-Intelligent-connectivity-report.pdf. Accessed 19 Jan 2023
17. Seeburn K (2019) 5G and AI: a potentially potent combination. Available at http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=1146#Comments. Accessed 20 Jan 2023
18. Drechsler et al (2020) At the crossroads between digital innovation and digital transformation. https://www.researchgate.net/publication/341412594_At_the_Crossroads_between_Digital_Innovation_and_Digital_Transformation. Accessed 20 Jan 2023
19. Kokolek et al (2019) Data protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en
20. Forradellas R, Gallastegui L (2021) Digital transformation and artificial intelligence applied to business: legal regulations, economic impact and perspective. https://www.mdpi.com/2075-471X/10/3/70. Accessed 19 Jan 2023
21. Fedrecheski G et al (2020) Self-sovereign identity for IoT environments: a perspective. In: 2020 global internet of things summit (GIoTS). IEEE
22. Harper KE, Ganz C, Malakuti S (2019) Digital twin architecture and standards. IIC J Innov 12(2019):72–83
23. Bhowmik D, Feng T (2017) The multimedia blockchain: a distributed and tamper-proof media transaction framework. In: 2017 22nd international conference on digital signal processing (DSP). IEEE
24. Bakre A, Patil N, Gupta S (2017) Implementing decentralized digital identity using blockchain. Int J Eng Technol Sci Res 4(10):379–385
25. Yaqoob I et al (2020) Blockchain for digital twins: recent advances and future research challenges. IEEE Netw 34(5):290–298
26. Vast R et al (2021) Artificial intelligence based security orchestration, automation and response system. In: 2021 6th international conference for convergence in technology (I2CT). IEEE
27. Ahmad I, Gurtov A, Kumar T, Liyanage M, Okwuibe J, Ylianttila M (2017) [online] Available at http://jultika.oulu.fi/files/nbnfi-fe201902124647.pdf. Accessed 23 Jan 2023
28. Yesuf AS (2017) A review of risk identification approaches in the telecommunication domain. https://www.researchgate.net/publication/314392917_A_Review_of_Risk_Identification_Approaches_in_the_Telecommunication_Domain [PDF] In: Conference paper. Conference: the 3rd international conference on information systems security and privacy—ICISSP. Accessed 20 Jan 2023
29. Reuters (2017) Cyberattack hits 200,000 in at least 150 countries: Europol https://www.reuters.com/article/us-cyber-attack-europol-idUSKCN18A0FX. Accessed 20 Jan 2023
30. Brewster T (2017) How hackers broke equifax: exploiting a patchable vulnerability. forbes. https://www.forbes.com/sites/thomasbrewster/2017/09/14/equifax-hack-the-result-of-patched-vulnerability/?sh=ce0ddce5cda4. Accessed 20 Jan 2023
31. Wang A (2018) 'I'm in your baby's room': a hacker took over a baby monitor and broadcast threats, parents say. Washington Post. https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/
32. Shu X et al (2017) Breaking the target: an analysis of target data breach and lessons learned. arXiv preprint. https://arxiv.org/pdf/1701.04940.pdf. Accessed 20 Jan 2023
33. Gara T, Warzel C (2014) A look through the sony pictures data hack: this is as bad as it gets. BuzzfeedNews. https://www.docketalarm.com/cases/PTAB/CBM2015-00030/Covered_Business_Method_Patent_Review_of_U.S._Pat._6321201/03-10-2015-Patent_Owner/Exhibit-2002-Exhibit_2002___A_Look_Through_The_Sony_Pictures_Data_Hack___BuzzFeed_News/

34. SDxCentral (2019) What are the top 5G security. Challenges". Available at https://www.sdxcentral.com/5g/definitions/top-5g-security-challenges/. Accessed 17 Aug 2019
35. Zhang Y (2018) Network function virtualization concepts and applicability in 5G networks, 1st edn. Wiley, New Jersey
36. Condoluci M, Mahmoodi T (2018) Softwarization and virtualization in 5G mobile networks: benefits, trends and challenges. Comput Netw 146(1):65–84
37. Huawei (2018) 5G security: forward thinking Huawei white paper. Available at https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf. Accessed 19 Jan 2023
38. Calder A, Watkins S (2015) IT governance: an international guide to data security and ISO27001/ISO27002, 6th edn. Kogan Page, London
39. Miller L (2016) IoT security for dummies, inside secure edition, 1st edn. John Wiley & Sons, Chichester/West Sussex
40. Blum JJ, Lawson-Jenkins K, Hoffman L-J (2006) Trust beyond security: An expanded trust model. Commun ACM 49(7):95–101
41. Fogg BJ, Tseng S (1999) Credibility and computing technology. Commun ACM 42(5):39–44
42. GOV.UK (2022) Cyber Security Breaches Survey 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022#chapter-5-incidence-and-impact-of-breaches-or-attacks https://www.ncsc.gov.uk/news/data-breach-500m-yahoo-accounts https://hoteltechreport.com/news/marriott-data-breach. Accessed 19 Jan 2023
43. Confessore N (2018) Cambridge analytica and facebook: the scandal and the fallout so far https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Accessed 19 Jan 2023
44. Aïmeur E, Schőnfeld D (2011) The ultimate invasion of privacy: identity theft. In: 2011 ninth annual international conference on privacy, security and trust. IEEE. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html Accessed 23 Jan 2023
45. Privacy International (2017) 101: data protection. https://privacyinternational.org/explainer/41/101-data-protection. Accessed 23 Jan 2023
46. Masombuka M, Grobler M, Watson B (2018) Towards an artificial intelligence framework to actively defend cyberspace. In: European conference on cyber warfare and security. Academic conferences international limited. https://search.proquest.com/openview/f6ccddd62973bd89da756a6c4f7272f0/1?pq-origsite=gscholar&cbl=396497&casa_token=fefF24OzjlcAAAAA:lW8TZptX9KGeshqbVXXBk1MBmrm0zyKHj5mmY62oPWdizJiYTe0WcDk4RMFtG2P0ZsuzdvAtZBo
47. Babiceanu RF, Seker R (2023) Big data and virtualization for manufacturing cyber-physical systems: a survey of the current status and future outlook. Computers in industry 81:128–137. https://www.sciencedirect.com/science/article/pii/S0166361516300471?casa_token=S59wxZXqps8AAAAA:SudkZGNExVlneS0cwzOiJPq3T6peQI63_K3I1fFNKuIkNz4hhlaAt4IKbxWnjFT9WBwX37vxlII. Accessed 22 Jan 2023
48. Hicks A et al (2019) Global mapping of citizen science projects for disaster risk reduction. Frontiers Earth Sci 7:226. https://doi.org/10.3389/feart.2019.00226/full. Accessed 19 Jan 2023
49. ISO/IEC (2022) https://www.iso.org/standard/82875.html
50. NIST (2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
51. ISO (2019) https://www.iso.org/standard/75106.html
52. BS (2007) https://knowledge.bsigroup.com/products/business-continuity-management-specification-1/standard
53. Schlehahn E (2020) Cybersecurity and the state. The ethics of cybersecurity. Springer, Cham, 205–225
54. Eltringham M (2017) UK organisations remain unprepared to deal with effects of cyber attack. UK organisations remain unprepared to deal with effects of cyber attack—Workplace Insight. Accessed 19 Jan 2023
55. Caulkins B, Marlowe T, Reardon A (2018) Cybersecurity skills to address today's threats. In: Ahram T, Nicholson D (eds) Advances in human factors in cybersecurity, AHFE 2018. Advances in intelligent systems and computing, pp 782–788. https://doi.org/10.1007/978-3-319-94782-2_18

56. Panda A, Bower A (2020) Cyber security and the disaster resilience framework. Int J Disaster Resilience Built Environ 11(4):507–518
57. Goodwin C et al (2015) A framework for cybersecurity information sharing and risk reduction. Microsoft
58. Landry BJL, Koger MS (2006) Dispelling 10 common disaster recovery myths: Lessons learned from hurricane katrina and other disasters. J Educ Resour Comput (JERIC) 6(4):6-es
59. Hyslop M (2007) Comments on standards in information security, disaster recovery, business continuity and business resilience. Crit Inf Infrastruct Resilience Prot (2007):94–144
60. Schmidt CG, Wagner SM (2019) Blockchain and supply chain relations: a transaction cost theory perspective. J Purch Supply Manag 25(4):100552
61. Pickles J, Zhu S (2013) The California transparency in supply chains act. SSRN Electron J. https://doi.org/10.2139/ssrn.2237437
62. Cheung K-F, Bell MGH, Bhattacharjya J (2021) Cybersecurity in logistics and supply chain management: an overview and future research directions. Transp Res Part E Logistics Transp Rev 146:102217. https://doi.org/10.1016/j.tre.2020.102217
63. Kendzierskyj et al (2021) Cyber security and supply chain management, pp 147–174. https://doi.org/10.1142/9789811233128_0007. Accessed 22 Jan 2023