5G human rights assessment

ericsson.com/
human-rights

March 2021

Contents

Executive summary

The rollout of 5G brings huge benefits — but crucial human rights risks also need to be addressed.

5G technology has the potential to enable a wide range of benefits for industries, consumers and society, as a result of increased connectivity. As is the case with any technology, however, there are crucial human rights risks associated with intended and unintended misuse.

Ericsson believes that access to networks and technologies that enable communication is a basic human need that underpins the principles of freedom of expression and opinion, and the free exchange of ideas and information. It also acknowledges its responsibility to respect human rights as articulated in the UN Guiding Principles on Business and Human Rights.

This responsibility entails continuously conducting human rights due diligence of its operations, products and services and business relationships. This human rights assessment is a crucial part of ensuring that risks and impacts are identified at an early stage of the 5G rollout, taking action to mitigate risks and address impacts where needed, as well as proposing ways of collaboration across the ICT industry.

Based on a comprehensive assessment methodology, extensive research and internal and external stakeholder consultations, Ericsson has identified a wide range of impact areas, divided into five categories:
1. Its own operations
2. Its supply chain
3. Its customer relationships
4. Involvement with governments
5. Broader societal impacts

Each category includes distinct impact areas and further analysis of the severity of the impact, how Ericsson is connected, and the actions needed to mitigate the risk.

The first section of this report covers how the assessment was conducted, and then moves on to an overview of the ICT industry and 5G technology.

The bulk of the report provides a detailed overview of the identified salient impact areas connected to 5G technology and Ericsson's business, concluding with a cross-cutting analysis of improvement areas and how the findings of the assessment will be embedded into company policies and procedures.

While Ericsson believes that this report is an important first step in taking responsibility for human rights issues connected to 5G technology, it acknowledges that additional efforts are required to effectively address the identified impact areas so far, and to be prepared to act when new issues emerge.

The aim of this assessment is to be a starting point for further engagement and learning. Customers, suppliers, non-governmental organizations (NGOs), investors and other stakeholders are invited to reach out and engage in a constructive dialogue to find joint ways of working on existing issues, as well as raise concerns on topics that have not been covered.

Ericsson is committed to its responsibility in the ICT ecosystem, and urges peers, partners and interested parties to join this effort.

Introduction

In this report, Ericsson takes an important first step, and proposes collaboration across the ICT industry to effectively address the identified impact areas, and prepare for emerging human rights issues.

Why a 5G human rights assessment?
Information and communication technology (ICT) is deeply integrated into our working and personal lives. Digital communication is more global, affordable and accessible than ever before, enabling billions of people to share ideas, acquire knowledge, improve their quality of life and boost livelihoods. ICT also promotes greater transparency and enhances many fundamental human rights — such as the right to health, education, freedom of assembly and freedom of expression.

Today, the role of ICT is an integral part of society, and its importance and prevalence will only increase in the years to come. Global 4G population coverage was around 80 percent at the end of 2019, while 3G coverage was around 95 percent. By the end of 2020, 5G population coverage is estimated to reach 15 percent, equivalent to over 1 billion people. By 2026, 40 percent of all mobile subscriptions globally are expected to be covered by 5G. Today, there are around 8 billion mobile subscriptions. This figure is estimated to increase to 8.9 billion by the end of 2025, of which 88 percent will be for mobile broadband.[1]

The scale and speed of this transformation is unprecedented. The evolving networked society, in which anything that can be connected will be connected, offers tremendous potential. As a recent example, the COVID-19 pandemic, requiring social distancing and keeping millions at home, has placed significant demands on infrastructure. Systems supporting healthcare, education and businesses of all types are under stress.

This massive disruption has highlighted the value of the network in enabling critical services to continue to function in providing a safer work environment for many by working remotely, and in ensuring ideas and opinions continue to be shared shared despite a global lockdown.

While the ICT infrastructure is a crucial part of our society, bringing benefits to users and communities, it is just as important to recognize the inherent risks of adverse impacts that a connected society brings. In particular, this relates to the potential for misuse of technology and unintended consequences. The same human rights that are enabled and strengthened through ICT could also be infringed and violated using this technology.

Ericsson has therefore decided, at an early stage of the 5G rollout, to conduct this Human Rights Assessment (HRA) to identify risks and potential impacts connected to the technology. While it continuously identifies, mitigates and addresses human rights risks connected to its business through embedded human rights due diligence processes, it is important to proactively recognize the potential for misuse and unintended consequences of new technology.

Additionally, as an industry leader and integral part of the ICT ecosystem, Ericsson has an important role in shaping developments in the industry through shared learning, best practice and the use of leverage. By identifying key risks related to its own operations, it also intends this HRA to be a springboard for constructive multi-stakeholder dialogue about ICT and human rights — with particular focus on emerging and increased challenges connected to 5G.

40%

By 2026, 5G is expected to cover 40 percent of all mobile subscriptions globally.

---

[1] Ericsson Mobility Report, June 2020 and November 2020

Objectives of the assessment

With the upcoming large-scale rollout of 5G technology, Ericsson wants to proactively take a human rights approach, by bringing an additional focus to the technology and how it can address potential negative impacts. 5G is groundbreaking technology, and core to Ericsson's future offerings. It is therefore important to understand the potential human rights impacts connected to it. This assessment looks at the potentially negative impacts of the technology from the perspective of affected stakeholders. It aims to identify mitigating actions and further stakeholder consultation needed to properly address the issues.

The aims of the assessment include identifying and prioritizing the most severe (salient) negative human rights impacts related to the emergence of 5G technology, understanding related stakeholder concerns and setting the internal strategy for preventing and mitigating potential human rights impacts over time.

Ericsson is keen to share learnings from the assessment with operators, global peers, industry initiatives and other interested parties, enabling collaborative approaches to addressing risks, demonstrating leadership on human rights and igniting momentum around these topics.

Companies can impact human rights in multiple ways, through their actions and decisions (or lack of action) and through their business relationships.

Companies can affect the human rights of their employees and contract workers, workers in their supply chains, communities around their operations and customers and end users of their products and services. For a more detailed overview of Ericsson's responsibility in connection to human rights impacts, see page 17.

Ericsson may be involved with 5G-related human rights impacts through its own activities (for example installing 5G base stations) and its supply chain (such as factory workers making/building hardware components for Ericsson technology), through to customers (such as misuse of technology for intrusive surveillance purposes). In most cases the impacts are not unique, or indeed solely attributable, to 5G technology (some already exist with 3G and 4G technology), but many are heightened due to the combination of 5G with other emerging technologies, such as Artificial Intelligence (AI), the Internet of Things (IoT), augmented reality (AR), Big Data and so on.

In many cases, impacts will occur in business relationships and Ericsson will work with mobile operators, governments and other parties to address these risks.

For each of these issues, there is a responsibility to "know" what the risks are and "show" what is being done to prevent and mitigate them. What follows in this report is an outline of the key risks identified through this process, along with initial suggestions for their mitigation.

Scope of the assessment
5G is not a limited set of technologies, but rather a new generation of communication and connectivity. It is therefore challenging to effectively limit the scope of this HRA to a specific set of products or offerings. For the purpose of this report, and in order to define a scope, we use the 5G definition as presented in the EU Commission Recommendation 2019/534.

This report is based on the understanding of the responsibility to respect human rights as laid out in the UN Guiding Principles on Business and Human Rights (UN Guiding Principles or UNGPs). The identified impact areas are within the scope of responsibility laid out by the UNGPs. It is clear that many of these areas are in need of collective, multi-stakeholder action. There are also likely to be additional impact areas that need to be addressed from a societal perspective, and Ericsson is committed to contributing to those where it can.

The scope of the impact areas is wide, covering its operations, supply chain, customer relationships and impacts on end users, as well as broader societal impacts. This HRA is, however, not a full company review of Ericsson, across all business and market areas, but focuses on 5G technology and rollout.

Ericsson has previously conducted country-specific human rights impact assessments, which have also informed the work on this report. Based on the findings of this assessment, additional country level HRAs will be conducted.

Methodology of the assessment
In this assessment, Ericsson collaborated with Shift, the leading center of expertise on the United Nations Guiding Principles on Business and Human Rights. Ericsson participates in Shift's Business Learning Program, and through this, Shift provides advisory support on implementation of Ericsson's responsibility to respect human rights as laid out in the UN Guiding Principles. For this 5G human rights assessment, Shift advised Ericsson on how to apply the lens of the UN Guiding Principles, including developing the methodology for conducting the assessment, analyzing the business and its involvement with human rights impacts, engaging expert and other stakeholders, facilitating internal cross functional workshops, helping to design creative ways to build and apply leverage and providing feedback on how to embed respect for human rights organizationally. The final report was written by Ericsson, with input from Shift.

Ericsson is committed to the UN Guiding Principles, which form the foundation of its human rights strategy and program. The methodologies used for this technology-based assessment, and those for the country-based assessments which preceded it, are intended to be aligned with the UN Guiding Principles.

> "5G networks means a set of all relevant network infrastructure elements for mobile and wireless communications technology used for connectivity and value-added services with advanced performance characteristics such as very high data rates and capacity, low latency communications, ultra-high reliability, or supporting a high number of connected devices. These may include legacy networks elements based on previous generations of mobile and wireless communications technology such as 4G or 3G. 5G networks should be understood to include all relevant parts of the network."[2]

[2] EU Commission recommendation 2019/534 of 26 March 2019 Cybersecurity of 5G networks

Guiding Principle 18 sets out that the initial step of a human rights due diligence process is to identify and assess how a company's activities and business relationships may pose risks to human rights.[3] The process involves considering the potential negative impacts of current and planned activities and business relationships on individuals and communities, and sets priorities for action to mitigate any such risk, based on the severity of the risk to people's human rights.

Through this process, businesses should pay particular attention to any human rights impacts on individuals or groups that may be at heightened risk of vulnerability or marginalization. Given the dynamic nature of business activity (particularly in relation to technology), assessments of human rights impacts should be undertaken at regular intervals, and ideally, prior to a proposed (new) business activity.

To enable businesses to assess their human rights impacts robustly, they should seek to understand the concerns of potentially affected stakeholders (people and communities whose human rights might be adversely impacted by business operations, products and services) by consulting with them directly. In the event that such engagement is not feasible, businesses should consider consulting reasonable alternatives, such as credible proxies who can provide insight into the perspectives of affected stakeholders, as well as independent experts who can bring particular knowledge or expertise in relation to specific issues, geographical contexts or other relevant matters.

Engaging with potentially affected stakeholders as part of an HRA of emerging technologies poses practical challenges. Firstly, it involves identifying who qualifies as a potentially affected stakeholder when technology, such as 5G, is so broadly used across sectors in society. Every user of mobile communication could potentially be an affected stakeholder.

Secondly, since the rollout of 5G is still in its early stages, most identified impacts will be potential. Based on this, it was decided to engage mostly with credible proxies, rather than individual users.

The assessment of human rights impacts informs subsequent steps in the human rights due diligence process.

[3] Human rights due diligence is defined as: "An ongoing risk management process that a reasonable and prudent company needs to follow in order to identify, prevent, mitigate and account for how it addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed."

**Table 1: How this assessment aims to implement guidance on HRAs
and subsequent action as laid out in the UN Guiding Principles**

Typical/necessary process element according to the UNGPs[4]	Implementation aims
Assess the human rights context prior to a proposed business activity, where possible.	Extensive research and consultation with internal and external experts on the nature of the 5G technology and rollout activities and plans.
Identify who may be affected.	Throughout the process, the assessment has identified and detailed specific groups of people that could be affected, such as supply chain workers, technology users, journalists, human rights defenders, Ericsson employees and contract workers (see page 23).
Pay special attention to human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalization.	Experts and civil society organizations were consulted to help identify specific groups of people that would be particularly vulnerable to impacts. Interviews conducted included individuals and organizations who are at risk and/or work directly with such groups.
Bear in mind different risks that may be faced by women and men.	Several experts and CSO organizations consulted have a specific focus and expertise on gender-differentiated impacts of wireless technology.
Include all internationally recognized human rights as a reference point.	The assessment has included all rights contained in the International Bill of Human Rights — meaning the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights and its two Optional Protocols. The assessment also included the principles concerning fundamental rights set out in the International Labour Organization's Declaration on Fundamental Principles and Rights at Work.
Catalog relevant human rights standards and issues.	For each identified risk to human rights, the specific internationally recognized human rights involved were identified, assessed and described.
Project how the proposed activity and associated business relationships could adversely impact the human rights of potentially affected stakeholders.	As a basis for the assessment, typical relationships and affected people (and the human rights at risk) in the 5G ecosystem were mapped and analyzed. Internal and external stakeholders were consulted on all aspects, including the severity and likelihood of impacts, and were asked to consider how existing and future 5G activities could have specific human rights impacts and how Ericsson would be connected to them.
Undertake at regular intervals.	While this is an initial broad assessment of 5G technology and its rollout, Ericsson intends to regularly revisit the assessment, taking into account new developments and insights.
Consult with affected stakeholders directly; or in situations where such consultation is not possible, consider reasonable alternatives such as consulting credible, independent expert resources, including human rights defenders and others from civil society.	Some of the civil society groups consulted are likely to face risks themselves. Many have direct engagement with affected groups and conduct extensive research into how technology in general, and 5G in particular, impacts on human rights. Further direct engagement with affected stakeholders will be part of the country-based assessments that Ericsson will continue, into which this assessment will be an important input.
Assessment of human rights impacts informs subsequent steps in the human rights due diligence process.	Ericsson has identified and developed, in consultation with internal and external stakeholders, appropriate actions to address the identified risks.

[4] See commentary to UN Guiding Principles, pages 18—19

Typical/necessary process element according to the UNGPs	Implementation aims
Where a business enterprise causes or may cause an adverse human rights impact, it should take the necessary steps to cease or prevent the impact. If the business enterprise has leverage to prevent or mitigate the adverse impact, it should exercise it. If it lacks leverage, there may be ways for the enterprise to increase it.	Many identified risks are likely to occur in relation to Ericsson's business partners, governments and other parties in its value chain. As a result, throughout the assessment and reflected in this report, Ericsson has considered how to build and apply leverage with partners in response to specific risks.
The horizontal integration across the business enterprise of specific findings from assessing human rights impacts can only be effective if its human rights policy commitment has been embedded into all relevant business functions. This is required to ensure that the assessment findings are properly understood, given due weight and acted upon.	Throughout the assessment and subsequent action planning, Ericsson has engaged a wide range of internal functions and business areas to inform and understand the risks and devise appropriate responses and actions. It also aims to ensure strong future involvement from relevant functions to identify and address 5G-related human rights risks on an ongoing basis.

Steps in the process

Desktop research
An initial landscape analysis of Ericsson's business and 5G technology was completed. Desktop research was conducted to compile a broad list of potential people-related impacts, along with an understanding of the status of industry discussions on each topic.

Interviews with internal and external expert stakeholders
In order to fully understand how people may be impacted, it is critical to incorporate into the assessment process the perspectives of those people whose human rights could be impacted by 5G technology. Only through dialogue, engagement and sharing of experiences can a full picture emerge of the human rights impacts that they may be experiencing.

Central to the assessment process is engagement with potentially affected stakeholders and experts and organizations who can credibly reflect these perspectives. In parallel with a range of internal interviews, gathering perspectives across the business, Ericsson and Shift also held interviews with a number of carefully selected experts and organizations such as the Global Network Initiative and Access Now, as well as follow-on interviews with select regional and local civil society organizations conducting research and outreach on digital and human rights. A list of interviews is contained in the appendix.

Workshop to identify key impacts and develop an action plan
Key insights from both the stakeholder interviews and the desktop research formed the basis of an initial analysis of impacts that were presented and discussed at a day-long Ericsson workshop attended by a broad cross-section of internal stakeholders. These included representatives from all business areas as well as group functions such as Technology, Legal Affairs, People (Human Resources) and Government Relations.

The analysis of each potential impact was tested with the group and further insights were gathered to help inform the prioritization of the issues.

Following on from the workshop some further, clarifying desktop research was conducted, as well as additional interviews with experts and civil society organizations to discuss an initial list of identified potential human rights impacts related to 5G. Based on the outcomes of the workshop and stakeholder dialogues, detailed internal discussions were also held to identify effective and viable actions to mitigate the risks, as well as plan for further engagements.

Ericsson's business and its responsibility to respect human rights

This section explores the workings of the ICT ecosystem, what 5G is, and its global impact; and assesses Ericsson's involvement with human rights impacts and the opportunities for applying leverage and building collaboration.

The ICT ecosystem

The ICT sector consists of a wide range of companies delivering products and services, such as mobile operators, network vendors, web-based platforms, component and hardware manufacturers and software developers. It is important to note that the telecom industry is highly regulated, requiring companies in the sector to comply with licensing and standardization requirements. Government authorities and regulatory bodies therefore also play an important role in the ecosystem.

The different actors share a strong degree of interdependence. However, the type of human rights risks they face — as well as their capacity to address them — may vary considerably, depending on their place and role in the value chain. Understanding these interdependencies, as well as the unique roles of each actor, better enables companies to effectively identify and address salient human rights risks and create opportunities to cooperate in addressing risks and exercising leverage.

In order to better understand the context in which Ericsson operates and is potentially involved with human rights impacts, the scope of the identified key impact areas (discussed in the next chapter), and the types of actions that are undertaken to address them, this section of the report provides an overview of the ICT ecosystem and the major actors within it.

Network vendors

Network vendors, such as Ericsson, provide fixed and wireless telecom network equipment, solutions and software, such as switches, routers and radio base stations. The role of the vendor is to build the infrastructure that provides the basis for all fixed and mobile communications. Network vendors do not deal directly with issues involving third-party requests, such as government demands to remove or block online content, requests for user information, or network shutdowns. The main customers of network vendors are mobile operators. Vendors are not consumer-facing.

Ericsson does not manufacture surveillance technology, but does enable lawful interception functionality through interfaces in our networks, when required by law. It is important to distinguish between lawful interception and intrusive surveillance technologies that enable mass surveillance. The former is a legally mandated and standardized interception capability, while the latter is often unregulated and allows for arbitrary surveillance.

Mass surveillance, in contrast to lawful interception, refers to the bulk access and/or collection of many users' communications without prior suspicion of individual targets. The basics of lawful interception are explained under the relevant impact area of this report.

Ericsson, headquartered in Sweden and founded in 1876, is one of the leading providers of ICT infrastructure. Its main customers are mobile operators, and it operates in more than 180 countries, with approximately 100,000 employees worldwide.

Ericsson's portfolio is divided into four business areas: Networks, Digital Services, Managed Services and Emerging Business:
- Networks — developing, delivering and supporting telecom networks by providing hardware, software and services
- Digital Services — enabling digitalization through services such as network management and operations, revenue and customer management, communication services, core network and network functions virtualization, infrastructure and application development and maintenance
- Managed Services — managing, maintaining and optimizing telecom networks and IT operations on behalf of customers
- Emerging Business — accelerating new and sustainable businesses beyond Ericsson's traditional core business; for example, through technologies such as AI, automation, IoT connectivity, virtual reality (VR)/AR and edge computing

Mobile operators

Mobile operators provide local and international telecommunications services to users; both voice and data, including internet access. Operators are granted licenses to operate and obtain spectrum allocation by governments in each country of operations, and therefore have ongoing relationships with governments.

The contracts to provide telecom services, between a government and the operator, typically include legal obligations to provide interception capabilities as part of the license to operate. Operators are also required to respond to government requests to remove or block online content, or temporarily shut down networks.

It is important to note that these requests and capabilities in many cases are used for legitimate purposes such as public safety, emergency response and crime prevention. It is, however, also possible to misuse the technology in ways that adversely impact human rights. This will be further explained in the "Detailed analysis of salient human rights impact areas" section (see page 24) of this report.

The necessary technology enabling such functionality is also highly standardized by regional and international standardization bodies.

Figure 1: The ICT ecosystem

Governments
Manage and allocate radio spectrum, set regulatory frameworks, establish laws for the ICT industry and have various enforcement mechanisms

Standardization bodies
Produce voluntary standards, rules and technical specifications for ensuring quality and interoperability for the ICT industry

Mobile operators
Provide telecommunications services to users

Connected industries
Increasingly utilize IoT devices, dedicated networks and AI solutions

ICT ecosystem

Network vendors
Build the infrastructure that provides the basis for all fixed and mobile communications

Hardware manufacturers
Produce devices such as mobile phones, laptops and tablets, as well as cars, home appliances and accessories

Third-party application companies
Offer entertainment, business, health and education apps. Downloaded by consumers to mobile devices, via marketplaces such as Apple Store and Google Play

Over the top companies (OTTs)
Provide internet-based services like search, email, banking and commerce

Over the top companies (OTTs)

OTTs include internet service providers, enterprise and security software developers, IT service firms and content providers offering internet-based services, including search, email, banking and commerce, social networking, content, location-based services and weather information, as well as a wide range of applications, databases, storage and cloud computing and software.

A distinction could be made between service/app providers that provide an app that the user downloads to the device, as opposed to one native on their device or which uses a browser and thus resides entirely in the cloud.

Hardware and component manufacturers

Hardware manufacturers produce devices such as mobile phones, laptops and tablets, as well as cars, home appliances and accessories, which are increasingly connected to the internet through 5G.

Such devices often include apps that need personally identifiable information, such as location-based services, to make optimal use of the functionality. With an increased number of connected devices, the additional amount of generated data can have human rights implications if not managed correctly.

The supply chain of hardware manufacturers is often complex and opaque, with several tiers of component manufacturers between the final assembly sites and the mining operations extracting minerals and metals vital for the functioning of the end products.

Third-party application companies

These companies offer apps in areas such as entertainment, business, health and education. They are downloaded by consumers to their mobile devices, via marketplaces such as Apple Store and Google Play. Many app providers rely on the use of personal information to provide and optimize services to users.

Connected industries

The current industry transformation towards smart factories and automation requires manufacturing sites, logistics and distribution centers to be connected, in order to secure reliable communication between a growing number of remote-controlled and autonomous robots and automated guided vehicles on the factory floors. Furthermore, companies in all sectors are increasingly using private, dedicated networks for internal communications.

This development means that other industries are also becoming part of the ICT ecosystem, and facing issues connected to data generated through IoT devices and dedicated networks, as well as questions of trustworthy AI.

> More devices and more data mean potential human rights risks.
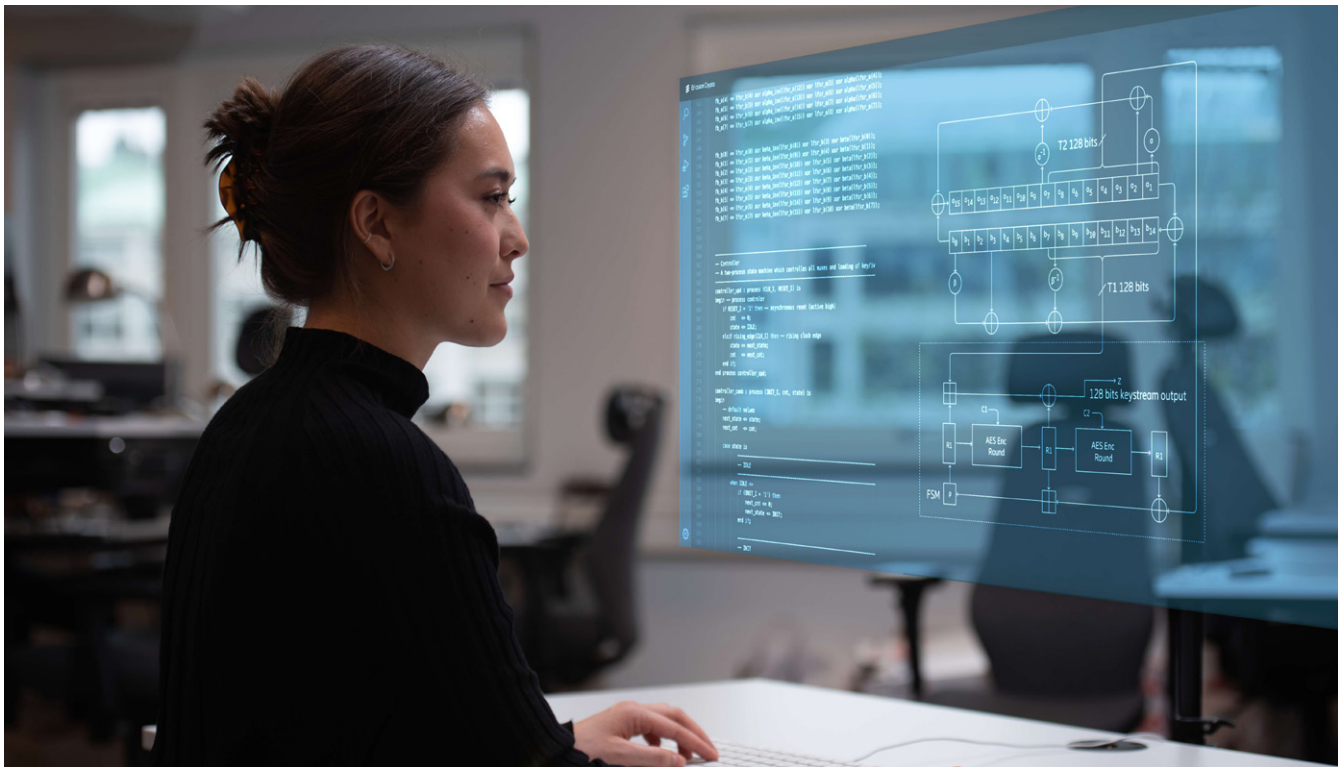
Governments

Governments set regulatory frameworks and establish laws for the ICT industry and have various mechanisms for enforcing such national laws. Mobile operators are granted a license to operate from the government. Despite widespread privatization of the telecom industry, some operators are still wholly or partly state-owned.

Government oversight primarily concerns services and content, not equipment, and therefore impacts operators and other service providers more directly than equipment vendors.

Governmental regulatory agencies are tasked with ensuring compliance with laws and regulations and establishing rules. Their role may include:
- implementing the authorization framework that allows companies and investors to establish new ICT businesses and provide ICT services
- regulating competition
- regulating network interconnection
- implementing universal service/access mechanisms to ensure the widespread (and affordable) diffusion of ICT

Managing and allocating the radio spectrum, law enforcement and first responders are integral to the government's role in the ICT ecosystem.

Law enforcement officers seek access to certain information in networks for the fulfillment of their duties, while first responders need critical location and other information to respond to emergencies.

Standardization bodies

National, regional or international organizations produce voluntary standards (a set of rules or technical specifications for ensuring quality and interoperability) for the ICT industry. These standards are essential to create global communication systems and ecosystems. Furthermore, technical standards, such as the specifications created by 3GPP (see below), enable the best technology to emerge and are key to ensuring robust choices for consumers and competition in the marketplace.

Standardization organizations relevant for mobile communications include:
- International Telecommunication Union (ITU) — a specialized agency of the United Nations responsible for all matters related to information and communication technologies
- 3G Partnership Project (3GPP) — a consortium of seven national or regional telecommunication standards organizations responsible for development and maintenance for 2G, 3G, 4G and 5G standards
- Internet Engineering Task Force (IETF) — an open standards organization developing internet standards, in particular the standards that comprise the internet protocol suite

Every three or four years, the ITU organizes World Radiocommunication Conferences to review and revise the international treaty governing the use of the radio-frequency

spectrum, while 3GPP organizes meetings almost monthly to prepare and discuss change requests against 3GPP specifications. These change requests may correct existing standards or introduce new functionality and include all aspects of mobile systems (including security standards to secure privacy and to prevent data loss and misuse).

Ericsson is actively participating in standardization bodies relevant for mobile communication systems and promotes open, transparent and consensus-based standardization processes.

7

3GPP is a group of seven telecom standards organizations responsible for developing and maintaining 2G, 3G, 4G and 5G standards.

What is 5G?

Each new generation of mobile networks has brought significant developments in how we communicate and the role digitalization plays in our society, and has enabled new business models to grow.

This section of the report provides an overview of how 5G works and highlights a number of use cases relevant for Ericsson, as examples of what 5G will enable.
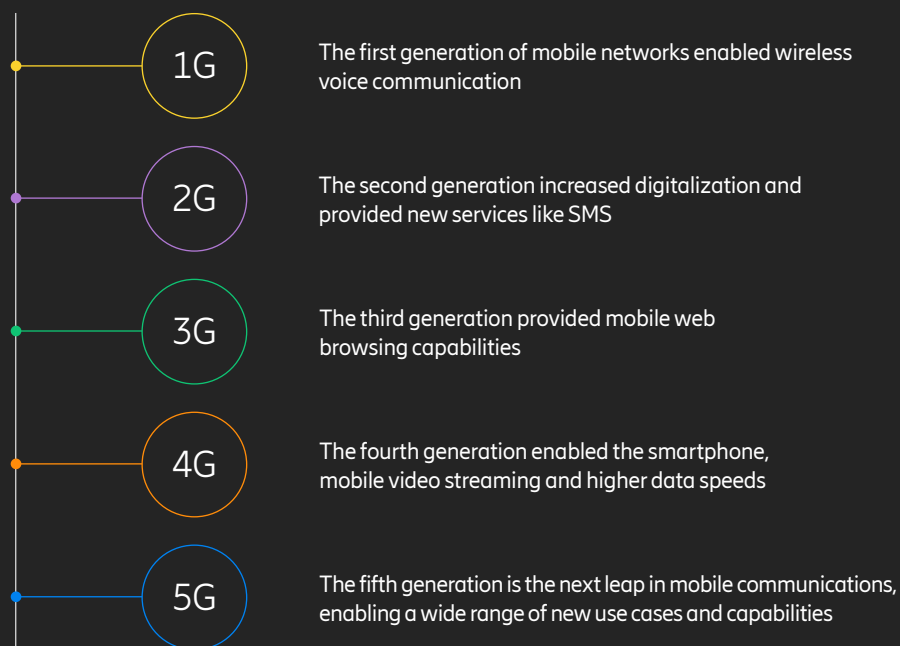
Overall, 5G will exponentially increase the capacity and efficacy of networks, compared to previous generations. Data will become the most important form of communication, rather than voice and SMS. Download and upload speeds will become considerably faster, and latency, or the time it takes devices to communicate with wireless networks, will also drastically decrease.

Spectrum

An important concept to understand when talking about mobile communication in general, and 5G specifically, is spectrum. Unlike previous generations, 5G operates on three different spectrum bands:

- Low-band spectrum is the primary band used today for 4G networks
- Mid-band spectrum provides faster speeds and lower latency
- High-band spectrum is also referred to as millimeter wave

Figure 2: Mobile network generations

1G — The first generation of mobile networks enabled wireless voice communication

2G — The second generation increased digitalization and provided new services like SMS

3G — The third generation provided mobile web browsing capabilities

4G — The fourth generation enabled the smartphone, mobile video streaming and higher data speeds

5G — The fifth generation is the next leap in mobile communications, enabling a wide range of new use cases and capabilities

Mobile telecommunications networks consist of four major domains:

The device — such as a smartphone, a tablet device or a router — is also called the user equipment

The core network (CN) provides coordination between different parts of the access network and connectivity to the internet
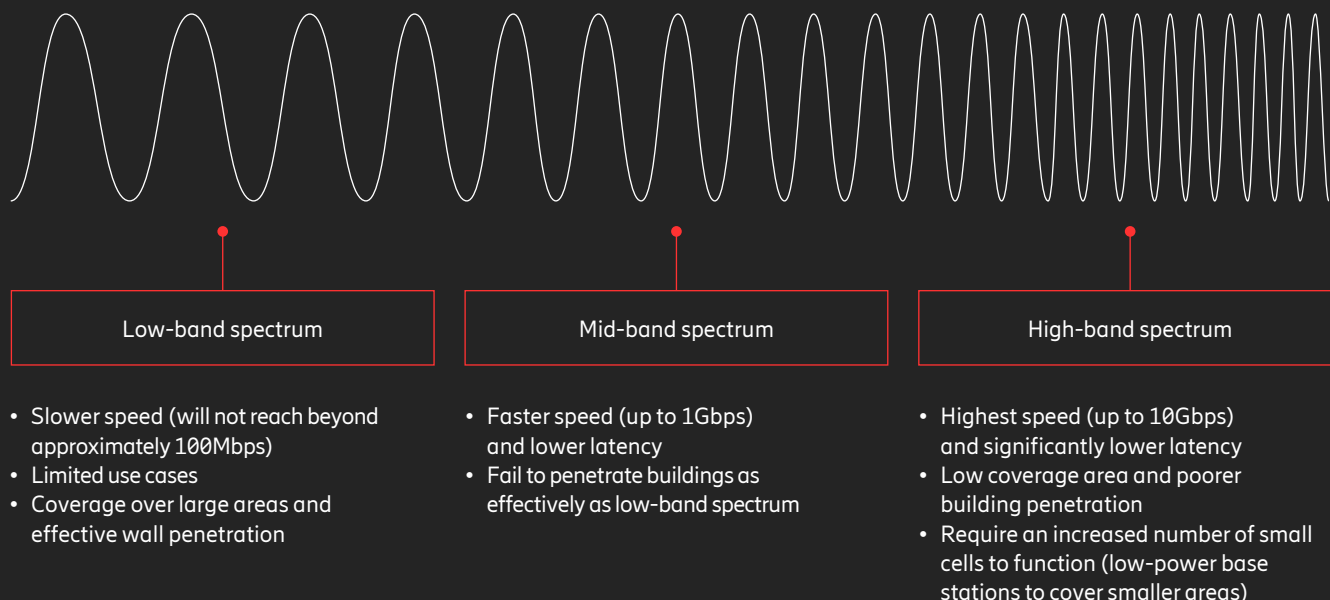
The radio access network (RAN) uses radio frequencies to provide wireless connectivity to the devices

The transport network provides connectivity between the RAN and the CN

Figure 3: Spectrum

Low-band spectrum	Mid-band spectrum	High-band spectrum
• Slower speed (will not reach beyond approximately 100Mbps) • Limited use cases • Coverage over large areas and effective wall penetration	• Faster speed (up to 1Gbps) and lower latency • Fail to penetrate buildings as effectively as low-band spectrum	• Highest speed (up to 10Gbps) and significantly lower latency • Low coverage area and poorer building penetration • Require an increased number of small cells to function (low-power base stations to cover smaller areas)

Use cases

Lower latency, faster data speeds and higher spectrum bands will enable new and enhanced use cases throughout society. Below are a few examples showcasing how 5G can be used.

Safer manufacturing through factory automation

With 5G Ultra-Reliable Low-Latency Communication (5G URLLC), automated assembly processes become more stable and reliable, while increasing the personal safety of factory workers. Humans and robots will be able to interact and work together; a machine can, for example, lift heavy objects, while the worker attaches components.

For this to work, the robot needs to be in constant communication with the factory, the workers and its surroundings. It needs to be mobile and have complete physical range of motion and environmental sensors.

The sensors will also detect if a factory worker reaches into their range and, due to low latency, instantly stop, thereby preventing injuries. This instant response with guaranteed reliability is not possible through traditional Wi-Fi or previous-generation mobile networks, meaning that such machines have historically required restrictive wired technology.

Automation in industries such as mining, considered a highly hazardous environment, can also reduce work-related injuries and fatalities, as well as reducing CO_2 emissions by increased efficiency of the vehicles.

Access to healthcare

From specialist oncology to simple ailment diagnosis, a large percentage of the world's population cannot reach or afford the healthcare professionals that they need to treat them. Higher bandwidth, low latency and network slicing can effectively contribute to increase specialist medical resources in remote regions. The ability to allow the remote transfer of haptic, tactile, audio and visual technologies enables a surgeon or doctor to perform a diagnosis or even surgery on a patient anywhere in the world. The principle of the solution is simple.

A doctor uses specialized haptic feedback gloves and VR equipment to operate on a patient via a robotic counterpart, potentially thousands of miles away. The gloves provide touch feedback from sensors on the robot arms, and the VR equipment places the surgeon in the same sensory environment as the patient. The combination of these two technologies removes both the obstacle of distance and the burden of travel cost, giving patients access to specialists, no matter where they are located.

The ideas of remote healthcare and robotic surgery are not completely new, but the introduction of 5G provides a new dimension and enables reliable communication that has the ability to perform mission-critical procedures.

For example, to operate safely, a surgeon needs to be able to react to physical and visual stimuli in under 10 milliseconds. When operating remotely, these stimuli will need to be delivered over a network, but the time required to compress and decompress video content vastly exceeds the safe reaction time. With 5G supporting the solution, these problems are sidestepped.

5G connectivity enables much greater bandwidth usage, while intelligent network slicing separates and prioritizes mission-critical functions, such as machine communication, which is required for the surgery. Most importantly, the low-latency attributes of 5G mean the haptic feedback is felt in near real-time through the surgeon's gloves.

Another use case within the healthcare sector is Narrowband Internet of Things (NB-IoT), which enables a wide range of devices and services to be wirelessly connected using cellular telecommunications bands. NB-IoT has broad practical applications, but one of the most crucial is how it can be used to improve standards of healthcare. With NB-IoT, equipment can be fully integrated via the cloud, which allows for enhanced data gathering and analysis and dramatically boosts machine efficiency and the reliability of network communications.

10ms

To operate safely, a surgeon needs to be able to react to physical and visual stimuli in under 10 milliseconds.

Autonomous vehicles
While self-driving vehicles will be made possible and safer as a result of lower latency in 5G, this is still some way in the future. Connected vehicle technology, on the other hand, is already becoming a vital part of road safety. Cellular technology has a role to play in reducing traffic incidents; human error is far more likely to cause accidents than overtly dangerous driving.

Cellular vehicle-to-everything (C-V2X) will enable vehicles to automatically respond to objects, such as road signs, hazards and people crossing the street, almost instantaneously. The use cases require near-immediate response times in order to increase safety outcomes on the road.

With an average 5G latency of 10ms, compared to 50—100ms for 4G, a car connected through 5G would for example significantly reduce the distance traveled before fully stopping, which could be the difference between life and death.

AR and VR
The COVID-19 pandemic has shown the need to interact, engage and stay connected, even in times of crisis. 5G will make AR and VR applications more immersive, far more interactive and accessible.

There are a wide range of AR/VR applications in different sectors, ranging from education to customer service and interactive meetings. By establishing a reliable and adaptable system through virtualization and software capabilities that enable high speed and low latency, 5G can allow tactile, visual and sound data to be shared in a way that combines immersive technology and physical existence.

The inclusion of network slicing can also guarantee specific resources to support the differing demands of each service or application. For instance, with the power of 5G, an expert mechanic can use tactile gloves when demonstrating how to replace a car engine; at the same time, the students can follow the expert via separate AR/VR goggles as if they are there in the same room. At work, we will be able to have virtual meetings where it appears as if two people are sitting together in a room, allowing for more interactive 3D experiences rather than today's video conferences.

These are just a few examples of what 5G will bring to industries, consumers and key societal functions. While the use cases presented aim at solving current-day challenges and provide clear

benefits to society, this report focuses on the risks associated with the technology. The next sections will elaborate on key impact areas, discuss potential mitigations and ways forward to ensure that the rollout of 5G does not bring unintended consequences of adverse human rights impacts.

Ericsson's involvement with human rights impacts[5]

The UN Guiding Principles, which form the basis for this assessment and for Ericsson's understanding of its human rights responsibilities, describe three ways in which a company can be involved with human rights impacts.[6]

1. It may cause the impact through its own activities.
2. It may contribute to the impact through its own activities — either directly or through another entity (government, business or other).
3. It may neither cause nor contribute to the impact, but be involved because the impact is caused by an entity with which it has a business relationship and is linked to its own operations, products or services.

The nature of a company's response in each of these three scenarios (cause, contribution, linkage) varies according to:

• whether the company primarily needs to change its own practices (when it causes that impact or it contributes to it), or to use leverage to effect change in the practices of a third party (contribution and linkage)
• whether the action required is solely forward-looking and preventative, or also includes remedying (or contributing to remedy for) past impacts

See page 31 for more detail of specific impacts Ericsson can be involved with and whether it causes, contributes to, or is linked to such impacts.

Expected response

Where a company causes a negative human rights impact, it should take the necessary steps to cease or prevent the impact and remediate it. While addressing such impacts will frequently be within a company's control, leverage may be relevant in certain instances, such as where a company is under pressure to take actions that would harm human rights (for example, by a government or by the purchasing decisions of a buyer).

Where a company contributes, or may contribute, to a negative human rights impact, it should take the necessary steps to cease or prevent its contribution and use its leverage with others to mitigate any remaining impact to the greatest extent possible. It should also take steps to ensure the remediation of any actual impact that has occurred, including in some instances by providing remedy to the extent of its contribution.

Where a negative impact is directly linked to a company's operations, products or services through a business relationship, the company has a forward-looking responsibility to seek to prevent the impact from continuing or recurring.

This business relationship may be a direct one, or with an entity more remote in the company's value chain. In a linkage situation, one of the most effective ways of deploying leverage may be to attempt to influence those that have caused the impact to provide remedy.

Ericsson's opportunities for applying leverage

Ericsson is expected to use its leverage where it is involved with an impact together with one or more third parties, or where an impact is otherwise directly linked to its operations, products or services through a business relationship. Leverage is defined as the ability to effect change in the wrongful practices of a third party that causes harm. In other words, leverage is a company's ability to influence the behavior of others.

Leverage is at the heart of what companies can realistically be expected to do when faced with complex human rights challenges. While a dominant or influential commercial position in a business relationship is likely to help a company's ability to use leverage, it is important not to consider leverage in purely commercial terms.

Many companies are likely to face situations in which they lack such a commercial position and need to think creatively about how to build sufficient leverage.

Ultimately, leverage is about creating the opportunity to change how people think and behave. In the context of the Guiding Principles, it is about changing the thinking and behavior of key people within a supplier, contractor, business partner, customer, client or government, where that organization's actions are increasing risk to human rights.

---

[5] Doing Business With Respect for Human Rights
[6] OHCHR's The Corporate Responsibility to Respect Human Rights: An Interpretative Guide New York and Geneva, 2012, p. 15

Table 2: How Ericsson uses leverage

Type of leverage	Existing or potential examples for Ericsson
A. Traditional commercial leverage: Leverage that sits within the activities a company routinely undertakes in commercial relationships, such as contracting.	For example, human rights expectations (aligned with the UNGPs) in supplier contracts and customer agreements and bidding processes.
B. Broader business leverage: Leverage that a company can exercise on its own, but through activities that are not routine or typical in commercial relationships, such as capacity building.	Offering human rights training to suppliers and/or other business partners and joint supplier-buyer assessments.
C. Leverage together with business peers: Created through collective action with other companies in or beyond the same industry.	Peer-learning initiatives such as joint action platforms for specific salient issues that are prevalent in the industry (for example privacy and surveillance, trustworthy AI).
D. Leverage through bilateral engagement: Generated through engaging bilaterally with one or more other actors, such as government, business peers, an international organization or a civil society organization.	Undertaking joint HRAs with an NGO, financier or export credit agency; collaboration with international union federation on labor rights; engaging a government on aligning ICT laws with human rights standards.
E. Leverage through multi-stakeholder collaboration: Generated through action collectively with business peers, governments, international organizations and/or civil society organizations.	Multi-stakeholder industry initiative (Global Network Initiative); supporting multi-stakeholder campaign for mandatory human rights due diligence legislation; engaging in multi-party initiative on strengthening responsible AI.

Thinking about leverage broadly
In determining what action to take, Ericsson can consider, in consultation with its stakeholders, the above listed types of leverage and select what type (or combination) could be most effective given a specific human rights risk in a specific situation.[7]

It can be helpful to identify specific moments in establishing and maintaining a business relationship when there may be a particular opportunity to exercise leverage, for example when a new customer or supplier agreement is being negotiated, provision of certain assistance or implementation of monitoring requirements, or when a complaint or grievance is logged and processed.

Where a company remains unsuccessful in preventing and/or mitigating the risks in its value chain, it needs to consider the following factors when thinking about ending a relationship on human rights grounds, where possible in consultation with relevant stakeholders:
• The severity of the negative impacts involved
• The extent to which the company has tried to use leverage and/or has run out of options for building further leverage
• Whether or not the relationship is a crucial one for the company (does it provide an essential product or service for which no reasonable alternative exists)
• Whether there would be other negative human rights impacts as a result of ending the relationship

Building the option for termination on human rights grounds into a relationship right from the start is an important source of leverage in itself and the threat of termination can, in some cases, be a powerful incentive for improved performance.

[7] The five types of leverage can be found in: Shift: Using Leverage in Business Relationships to Reduce Human Rights Risks, New York (2013)

Salient human rights issues related to 5G

Salient human rights issues discussed in this section may be affected by the rollout of 5G. Ericsson has identified key areas ranging from job impacts, to accidents and the misuse of personal data.

What are salient human rights issues?[8]
Human rights impacts are the most acute social, environmental and economic impacts a company can have on people, negatively impacting on their enjoyment of certain of their human rights. Salient human rights issues are in turn the most severe human rights impacts. They stand out because they are at risk of the most severe negative impact in connection with the company's operations or value chain. They are the human rights priorities for the company. They need the most urgent attention to prevent actual harm from happening, or to manage the harm that has occurred.

In practice, impacts that rise to this level of severity converge strongly with risk to the business, as seen in the many instances where they lead to reputation-damaging campaigns, disruption and delays to operations, increased costs of managing conflict, litigation and other costs or loss in value to the business. This is particularly evident over the medium to long term. The idea of "salience" is central to the UN Guiding Principles on Business and Human Rights, which are the global standard in this field. To identify a company's salient human rights issues, a company needs to map out the various impacts it could be involved with across its operations and value chain. It then identifies which impacts would be most severe by assessing how grave they would be (the scale of the impact), how widespread (the scope) and how difficult the impact would be to put right (remediability).

A secondary factor in the determination of salient human rights issues is the likelihood of these impacts occurring, by examining the business environment, business relationships, the type of business activity and the prevalence of vulnerable groups of people. The most severe issues that have the greatest likelihood of occurrence are the ones that the company should prioritize for action, although a low-likelihood, high-severity impact should be among the salient issues.

The assessment should be informed by an understanding of the perspectives of those people who could be impacted, and conclusions should be tested with stakeholders inside and outside the company. Once a company understands its salient human rights issues, it has taken a key initial step towards implementing the UN Guiding Principles.

The concept of "salience" provides companies with a robust method for identifying the most important human rights issues, assessed through an understanding of what the company does, where it works and who it works with, and informed by, but not derived from, the views of the most relevant stakeholders. Given the strong convergence between the most severe impacts on people and risks to the business, this method can also identify issues that are "material" to the business under most definitions, provided they take a medium- to long-term view.[9]

Salient human rights impacts identified for Ericsson's 5G business
In the course of the assessment, a number of salient human rights issues were identified.
- Salient risk areas: Among the many potential impacts and human rights issues identified, there were some impacts that could be grouped together in similar categories (such as health concerns, privacy, data loss and misuse), which we termed human rights risk areas.
- Potential impacts: Within each risk area, the impacts that were identified during the process are categorized.
- Human rights affected: Most identified impacts potentially affect multiple specific internationally recognized human rights. These are described in detail in the "Detailed analysis of salient human rights impact areas" section (see page 24) of this report and in a non-exhaustive overview table for each risk area.
- Potentially impacted people: Where possible the specific individuals or groups of individuals have been identified. These are again described in detail in the "Detailed analysis of salient human rights impact areas" section and in the following tables.

[8] UN Guiding Principles
[9] Salient Human Rights Issues

Figure 4: Human rights risk areas and impacts

Livelihoods/job transitions

Health concerns

Supply chain impacts

Privacy, data loss and misuse

Human rights
risk areas

Broader societal impacts

Network surveillance
and shutdowns

Network segmentation
and differentiation

Security and critical networks

01 Livelihoods/job transitions

5G is likely to accelerate the replacement of workers by machines

Significant portions of the working population can be impacted in the future, as 5G enables machines/robots to take on more specialized and professional work (not simply unskilled jobs on factory floors).

5G-enabled technology requires different skills

New technologies, enabled through 5G, will make many white-collar jobs redundant and/or requiring new skills that not all current Ericsson employees, contract workers and other staff may yet possess.

02 Health concerns

Workplace accidents related to installation of 5G equipment

Not new to 5G, health and safety risks facing Ericsson employees and many subcontractors arise in connection with the work involved in the physical rollout of 5G, specifically issues relating to working from heights and with electricity and road safety.

Perceived health risks related to 5G radio waves

While Ericsson, the wireless industry, expert bodies such as the World Health Organization and governments are confident, based on extensive research, that there is no established link between adverse health effects and radio waves from mobile communication equipment, perceived health risks exist and need to be addressed.

03 Supply chain impacts

The manufacturing of 5G hardware includes existing risks in the supply chain

This mainly concerns labor rights, including working conditions, bonded labor and the prevalence of migrant workers in factories in Ericsson's supply chain related to hardware manufacturing.

5G will increase demand for specific minerals, potentially from conflict-affected/high-risk areas

5G will result in increased use of lithium batteries, which contain nickel and cobalt.

04　Privacy, data loss and misuse

Increase of IoT will lead to increasing amounts and storage of personal data that can be abused

Data generated from social media, apps and the "ubiquitous connection" of IoT devices will generate a huge amount of personal information that is extractable by authorities. This could be used for legitimate law enforcement or other public policy purposes, or it could be used to abuse human rights.

Personal data can be sought by unscrupulous private and public actors

Key to the concerns are the myriad ways in which businesses will potentially seek access to specific and highly personal, sensitive information, in order to predict and monetize future behavior, potentially without the users' express knowledge. This may exacerbate existing risks to already at-risk users, including children.

05　Security and critical networks

Attacks on critical infrastructure will expose people who rely on them to severe risks

Critical infrastructure such as water utilities and power (nuclear, gas, hydro) will increasingly be connected through 5G. The risk of a cybersecurity attack on any of these installations could potentially also have significant repercussions for communities' human rights. While this threat is not new to 5G, it will be important to analyze how application of 5G technology in critical infrastructure poses risks to human rights.

06　Network segmentation and differentiation

Network slicing enables more private networks, linking them more closely to any company abuses

Private networks are already being built to support, for example, mining operations and smart factories. 5G becomes a more integral part of running such businesses, which makes the networks more closely linked to potential adverse impacts that these business relationships may be involved with.

Segmented networks could facilitate human rights abuse by governments

Private networks will increasingly become mission critical for government agencies. Such networks are primarily for the purpose of internal communications, but can nevertheless be a vital part in enabling an agency's activity, creating a link to potential human rights impacts as a result of the government's actions.

Network segmentation may affect net neutrality

The concerns related to net neutrality are that the increased possibilities of network slicing in 5G networks could lead to differentiation in offerings, and impact on the ability of users to utilize certain critical services fully. This could, for example, lead to reduced ability to: access online education platforms (affecting children's development, among other impacts), access basic and/or critical information and services (such as doctor appointments), or effectively do a job remotely.

07 Network surveillance and shutdowns

5G may increase some surveillance capabilities, including more precise geolocation data

The shorter-range 5G radiofrequency waves require a higher number of small cells, which may enhance the ability of a service provider to pinpoint the location of a device user. This change could place people already at increased risk in a potentially more vulnerable position.

Networks can be shut down in discrete ways providing more tools for governments to target specific groups

5G technology, with its potentially denser deployment of cell towers, may give governments more tools to request service providers to shut down highly discrete parts of the network. For example, targeting a single apartment building, office or indeed parts of a country populated by an ethnic minority.

08 Broader societal impacts

Uneven rollout of 5G may lead to (or exacerbate) the digital divide and other inequalities

Uneven distribution in the access to, use of or impact of ICT between any number of distinct groups could further be accelerated by 5G. Such "groups" may be defined based on social (including generations), geographical or geopolitical criteria, or otherwise, including between different countries and parts of the world, as well as within countries.

Trustworthy AI

There is a need to ensure that rights-respecting, ethical principles and regulations guide the development of AI in order to mitigate against a host of unintended negative consequences (many of which likely remain unidentified today), such as bias, discrimination and invasion of privacy.

Figure 5: Non-exhaustive overview of specific human rights and people that could be impacted for each risk area
Note: This should be read concurrently with the "Detailed analysis of salient human rights impact areas" section (see page 24).

	Livelihoods / job transitions	Health concerns	Supply chain impacts	Privacy, data loss and misuse	Security and critical networks	Network segmentation and differentiation	Network surveillance and shutdowns	Broader societal impacts
Human rights affected								
Privacy				●	●	●	●	●
Freedom of thought				●				●
Freedom of expression				●	●	●	●	●
Life and security		●	●	●	●	●	●	
Health and safety	●	●	●	●	●	●	●	
Just and fav. cond. of work	●	●	●					
Trade union rights	●	●	●					
Adequate standard of living	●	●	●	●			●	●
Non-discrimination	●	●	●	●			●	●
Conflict-related human rights			●				●	●
People potentially affected								
Employees	●	●		●	●	●	●	
Contract workers	●	●		●	●	●	●	
Supplier workers	●	●	●	●				
Communities		●	●	●	●			●
End users (in general)		●		●	●	●	●	●
Additional impacts on specific groups								
Journalists				●	●	●	●	
Human rights defenders			●	●	●	●	●	●
Political opponents				●			●	●
Ethnic minorities				●		●		●
Women			●	●		●		●
Children				●		●		●

Detailed analysis of salient human rights impact areas

This section explores Ericsson's own operations, suppliers, customers, involvement with governments and broader societal impacts, and how they relate to human rights risks.
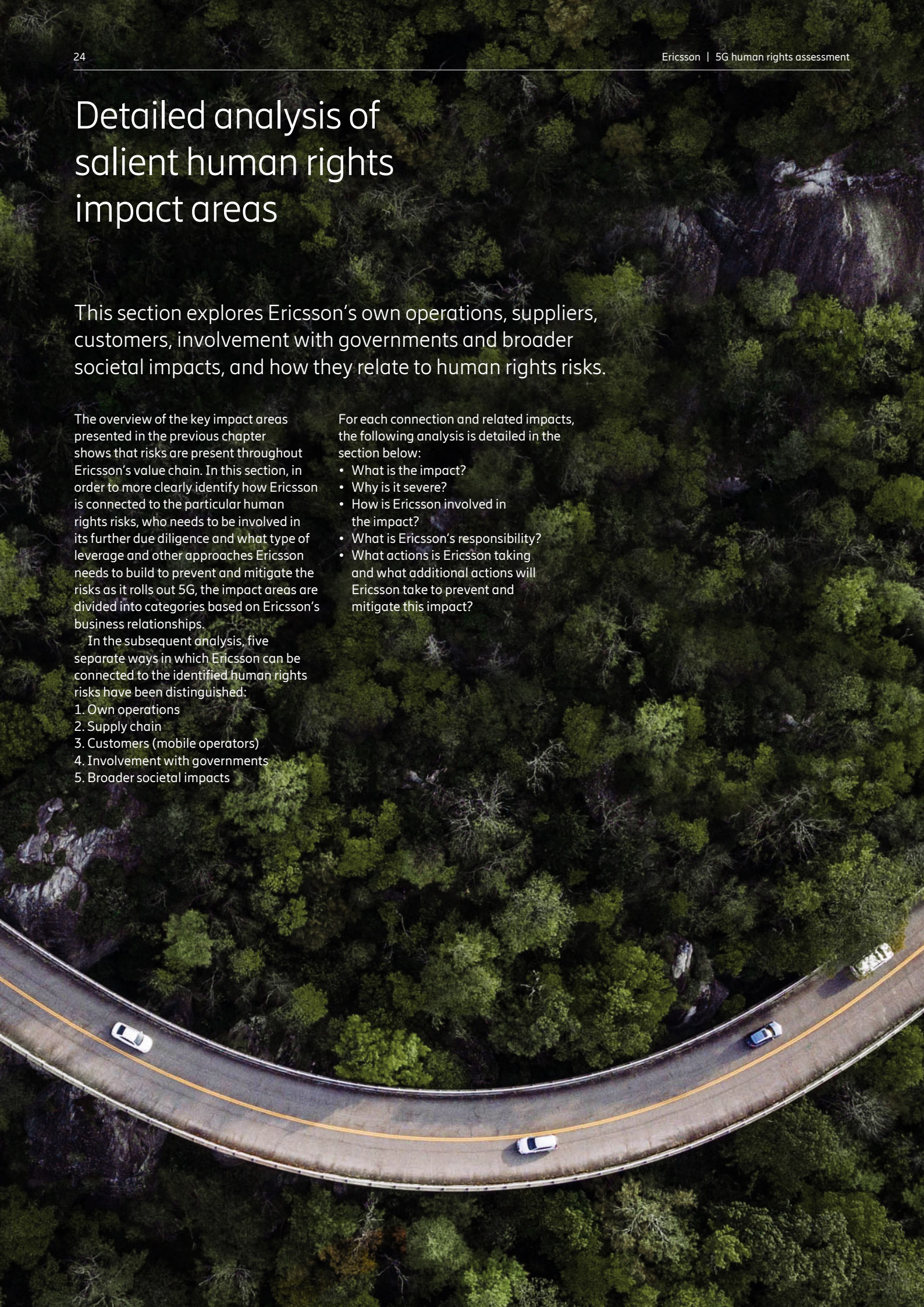
The overview of the key impact areas presented in the previous chapter shows that risks are present throughout Ericsson's value chain. In this section, in order to more clearly identify how Ericsson is connected to the particular human rights risks, who needs to be involved in its further due diligence and what type of leverage and other approaches Ericsson needs to build to prevent and mitigate the risks as it rolls out 5G, the impact areas are divided into categories based on Ericsson's business relationships.

In the subsequent analysis, five separate ways in which Ericsson can be connected to the identified human rights risks have been distinguished:
1. Own operations
2. Supply chain
3. Customers (mobile operators)
4. Involvement with governments
5. Broader societal impacts

For each connection and related impacts, the following analysis is detailed in the section below:
- What is the impact?
- Why is it severe?
- How is Ericsson involved in the impact?
- What is Ericsson's responsibility?
- What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?
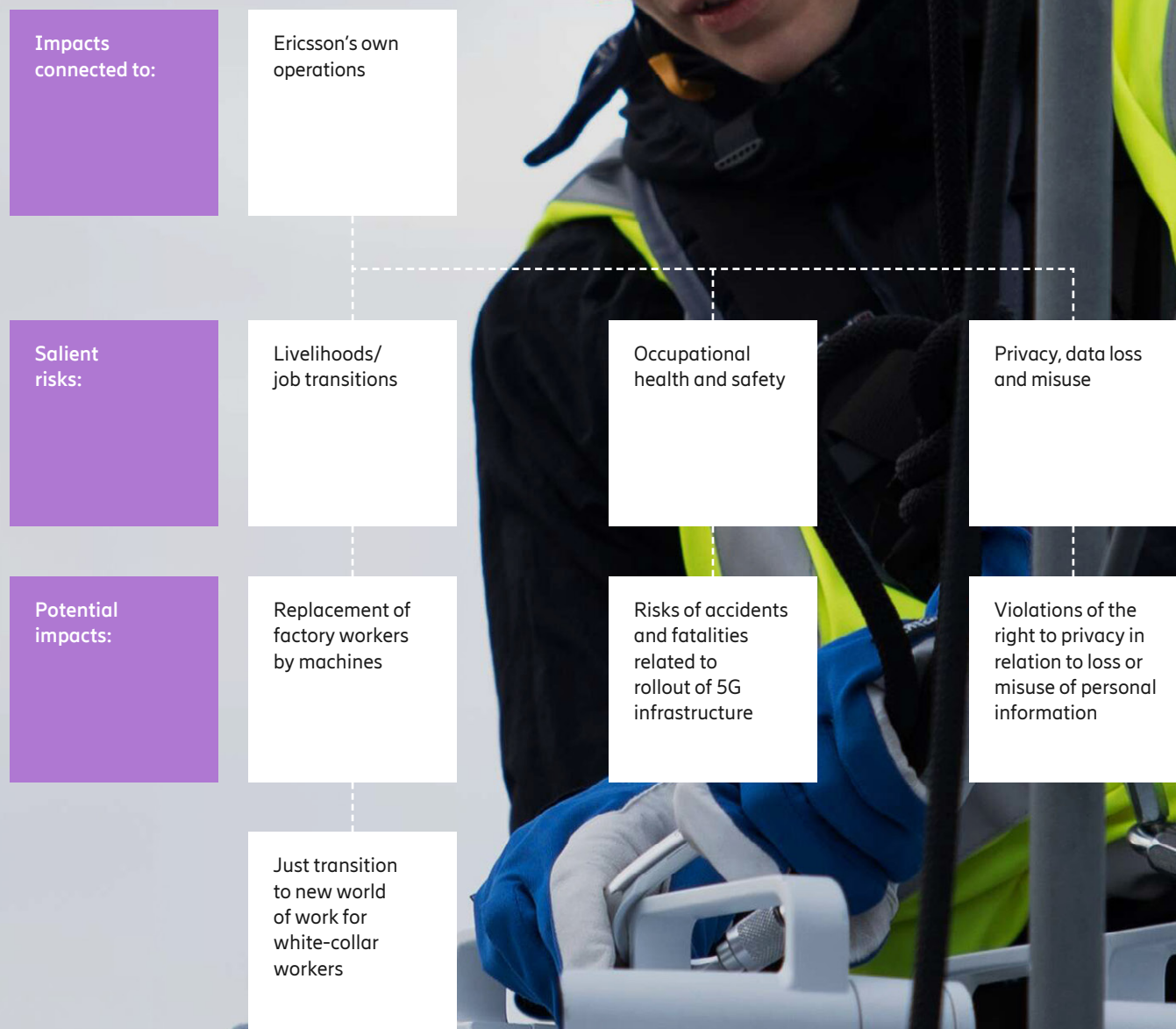
Ericsson's own operations

Impacts connected to:	Ericsson's own operations		
Salient risks:	Livelihoods/ job transitions	Occupational health and safety	Privacy, data loss and misuse
Potential impacts:	Replacement of factory workers by machines	Risks of accidents and fatalities related to rollout of 5G infrastructure	Violations of the right to privacy in relation to loss or misuse of personal information
	Just transition to new world of work for white-collar workers		

Table 3: Livelihoods/job transitions

Replacement of factory workers by machines	
What is the impact?	Ericsson has its own manufacturing and assembly sites in Brazil, China, Estonia, India, Mexico, Poland, Romania and the US. As manufacturing processes become more automated and efficient, enhanced by AI/ML and the availability of 5G technology (specifically, the ability of factories to run their own private cellular network), the opportunity for businesses to eliminate operating expenses (opex), including people-related costs, becomes very tangible. In this scenario, the risk to people could lead to shop floor factory workers being made redundant and being replaced by automated processes/machines. Over time, leaps in technological automation may lead to the replacement of skilled Ericsson workers by machines. While embracing technology in this way may result in improved occupational health and safety conditions for the remaining workers, due to the elimination of dangerous tasks from the factory floor, many people will likely lose their jobs or see their livelihoods at serious risk.
Why is it severe?	Losing jobs and livelihoods has the potential to severely impact thousands of Ericsson factory workers, gravely impacting a number of their rights, such as the right to just and favorable conditions of work and the right to an adequate standard of living. Work and income are important pre-conditions to the fulfillment of other rights, such as the right to food, health, family life and so on. Additionally, unemployed, unskilled or low-skilled workers will face difficulty in finding a replacement job without skills training. Over time, even highly skilled workers/employees may find it difficult to secure a new job as AI capabilities scale up and deployment costs reduce. Long-term unemployment can potentially lead to further negative impacts such as mental health issues.
How is Ericsson involved with the impact?	Ericsson owns and operates the manufacturing sites where these impacts may occur, where unions and governments are relevant parties to engage in social dialogue and provide retraining programs. Special attention is warranted for workers that are employed through third-party agencies at the sites, who may be at increased risk, and where Ericsson may be contributing to impacts and have less control to address the risks. This risk is likely to be more severe in countries with weak social protections by the government.
What is Ericsson's responsibility?	Ericsson has a responsibility to timely identify and address the adverse impacts arising from its business decisions; in particular to provide workers with sufficient warning and progressively manage people's transition to new jobs, especially the most vulnerable groups of workers that may not be able to make the transition on their own (including temporary and contract workers). This should involve engaging with legitimate representatives and is likely to involve providing and/or organizing and advocating for appropriate skills training for these workers.

Replacement of factory workers by machines	

What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson should undertake an analysis to determine which roles across the business (not just the more obvious roles such as factory shop floor workers) are vulnerable to elimination resulting from technology developments, in the near- and longer-term future.
	• This analysis should further identify which groups of workers may be most vulnerable for these impacts and include the following steps:
	  • In advance of any changes being shaped and implemented, organize a formal consultation process with the potentially impacted workers and their representatives (such as trade unions) to present the rationale for the decision, the timelines under consideration and share and discuss plans for how best to put the transition in place. This consultation process should be informed and guided by collective bargaining agreements and could include a series of group discussions with the broader impacted team, along with individual conversations with the impacted workers, providing them with the opportunity to air their concerns in private.
	  • Ericsson will develop plans to support vulnerable workers, including skills training and job transition. This could include assessing individual skills and strengths, determining if there are opportunities for redeployment to other parts of the business. Where this does not exist, Ericsson could investigate the potential for workers to secure similar kinds of work in other companies in the area (so that they would not have to involuntarily travel significant distances).
	  • Ericsson needs to engage with its third-party labor providers to address similar challenges with respect to its flexible workforce. Where necessary, it could build additional leverage with such parties to address impacts on the most vulnerable workers.
	  • The potential for workers to be impacted in relation to sophisticated automation is a trend across the industry and will become a broader business trend in the years ahead. In order to address systemic causes, and build leverage to achieve scalable solutions, Ericsson can also engage with relevant governments (national and local) and trade unions where job cuts will be made, explaining the forecast and the need to provide retraining and potentially economic diversification and advocate for social security provisions.
	  • Ericsson can also have a role to play in engaging with industry peers and international trade union organizations, in an effort to find appropriate and systemic responses involving training/reskilling programs and changes to secondary and third-level education curriculums, in order to meet future job and skills demands.

Table 4: Livelihoods/job transitions

Just transition to new world of work for white-collar workers	
What is the impact?	New technologies, including 5G, AI and others, are going to make many jobs redundant and/or require new skills (such as research and development and AI solutions) that not all current employees, contract workers and other staff may possess (yet).
Why is it severe?	Ericsson employs workers, including through third-party contractors, in network management centers that may become increasingly redundant as networks are managed through AI and related technologies. Also, many of Ericsson's business areas will need to evolve as 5G is rolled out, to continue to add value to the business. While for many this may be a common feature of their careers, for others it may not bring the same opportunities and for yet others it may pose significant risks to their employability and livelihoods leading to potentially significant related impacts.
How is Ericsson involved with the impact?	A decision by Ericsson to replace jobs that are currently performed by humans, with machines and AI technology, could involve Ericsson causing human rights impacts on workers. This impact could occur in relation to positions currently undertaken by Ericsson's own employees in the various business areas and functions, as well as long-term contractors and consultants supporting those areas; employees and third-party workers in network centers; or other Ericsson operations that are supported by subcontractors with significant numbers of people. Again, increased risk is likely to occur in countries where there are low levels of social protection and where there are not many affordable outside programs to retrain and reskill workers.
What is Ericsson's responsibility?	Ericsson has a responsibility to consider impacts for these workers on their livelihoods, in particular for the most vulnerable groups, and develop plans to prevent and mitigate impacts on them. Engagement and collaboration with trade unions is a crucial step in this process.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• As a first step, Ericsson should map — short, mid and long term — which workers are going to need to transition to new types of work, requiring new skills, including workers that are employed through third parties or subcontractors (in collaboration with those contractors). • Subsequently, identify those groups of workers that are particularly vulnerable, including contract workers, workers in countries with fewer social protections, with limited options for affordable retraining or jobs for which no easy transition can be made. • For Ericsson employees a transition plan should be developed to move them as much as possible to new positions and jobs, in consultation with workers and worker representatives. • Additionally, Ericsson needs to engage with contracting agencies to plan as far as possible in advance, identify groups at particular risk and work jointly to put in place appropriate mitigation plans, including through engagement with potentially affected workers and their representative unions. • Where necessary, also engage with governments, peers, unions and others to help shape and plan for the future technology "world of work" that is aligned with the responsibility to respect human rights.

Table 5: Occupational health and safety

Risks of accidents and fatalities related to rollout of 5G infrastructure	
What is the impact?	A significant portion of injuries and fatalities related to Ericsson's business stems from incidents during field activities to install, dismantle and manage radio towers and related equipment. Additionally, manual handling of products is an increased risk in the rollout of 5G, due to the size and shape of 5G products. This concerns both Ericsson's own employees as well as subcontractors across the world that are engaged in these activities. This risk is not new, and indeed Ericsson has implemented strong occupational health and safety measures to mitigate the risks.
Why is it severe?	In general, installing radio products and related equipment involves high-risk safety activities, including working with electricity, climbing and working at heights. The possible related impacts are of a grave nature, including loss of life, long-term injuries and health impacts and resulting impacts on livelihoods and families, in particular in countries lacking decent personal or health insurance or social protections for workplace-related incidents. Putting those grave risks into the context of a highly competitive international 5G rollout could potentially have impacts in several geographies.
How is Ericsson involved with the impact?	Ericsson-employed field personnel and subcontractors carry out this work across many countries. In addition, specialized agencies provide a range of these services to Ericsson, varying in nature depending on the country. In cases where Ericsson knows or should know about poor health and safety practices of subcontractors and does not implement credible measures to address the risks, it could be seen to be contributing to impacts.
What is Ericsson's responsibility?	Ericsson's responsibilities include ensuring a safe working environment and culture by implementing a health and safety management system that includes training, tools and processes to perform work safely. Ericsson has a system in place for reporting, analyzing and investigating incidents and a grievance channel that enables its workforce or anyone to raise issues. Ericsson works closely with its subcontractors to advance all of these systems in the same way and with the same level of seriousness and effectiveness.
What actions is Ericsson taking, and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson already manages health and safety risks closely and implements a strong set of mitigating measures across the business. Ericsson applies the same level of health and safety requirements globally, internally and in relation to subcontractors. These measures include a proactive approach to identify and mitigate risks, a system for investigating incidences, a grievance channel that enables its workforce and subcontractors to raise issues and the provision of appropriate remedies for workers who sustain injuries. Ericsson will maintain the strong focus on these risks and decrease the number of major incidents and fatalities. • Ericsson has approved a new target to reach zero fatalities and lost workday incidents by 2025. This applies to employees, subcontractors and suppliers. • Ericsson is in the process of developing a new global Environmental Health and Safety Tool, in order to more effectively monitor performance and compliance metrics. • Ericsson's deployment of a global wellbeing framework and program and the transition to ISO 45001 with a focus on leadership and employees' participation and consultation, will increase workforce engagement and awareness. • Find out more about our approach to occupational health and safety.

Table 6: Privacy, data loss and misuse

Violations of the right to privacy in relation to loss or misuse of personal information	
What is the impact?	Ericsson collects and holds data that includes personal information of employees and other workers. Additionally, Ericsson processes end-user data for its customers. This data handling is not new to 5G. If such data were to fall into the wrong hands, it could be exploited by third parties for instance for blackmail. In addition, in some jurisdictions it may be expected or even required for companies to log certain personal information that poses risks to human rights, such as someone's ethnicity, religion, gender or marital status. Governments or other actors could seize such information and use it for persecution or other illegitimate purposes.
Why is it severe?	Databases with personally identifiable information often contain the data of large numbers of people. Loss of such data can lead to identity theft, blackmail or the public sharing of sensitive information. Governments or other third parties might want to abuse such information and impact not only privacy rights but also a broader set of human rights, particularly in relation to vulnerable groups.
How is Ericsson involved with the impact?	In case of impacts, third parties violate the actual rights, but if Ericsson is not taking adequate and proactive measures to protect data and consider privacy and related risks of individuals, then it is at risk of contributing to these impacts.
What is Ericsson's responsibility?	Ericsson needs to make sure it has in place — and implements — effective privacy and cybersecurity policies to respect the right to privacy in all contexts and for all people it holds data on. Where Ericsson is processing data of end users (on behalf of mobile operators or other customers), this risk and needed measures would equally apply. Ericsson has a responsibility to make sure that data is well protected and that it proactively identifies risks to privacy and related risks. In particular, it should comply with the European Union General Data Protection Regulation (GDPR) and related standards and consider rollout across all its operations. In addition, it should specifically identify privacy risks in each jurisdiction of operation and proactively assess and manage risks to people that are particularly vulnerable, such as women in certain countries, LGBTQI individuals in many countries and ethnic and other minorities.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson recently strengthened the Group Privacy Compliance Office and Product Privacy Office and its focus on the implementation of the privacy compliance framework, closely connected to other ongoing compliance activities as well as Group Security and Product Security frameworks. • As part of this, Ericsson has established a global privacy strategy, which includes GDPR requirements as a baseline for global processes, which can be adapted where locally required. Related to regulatory developments, like the Schrems II decision,[10] Ericsson is constantly assessing privacy impacts and adjusting processes where needed. • Find out more about Ericsson's approach to privacy.

---

[10] Schrems II decision — InfoCuria

Ericsson suppliers

Impacts connected to:

Ericsson suppliers

Salient risks:

Supply chain impacts

Minerals from conflict-affected and high-risk areas

Potential impacts:

Labor rights risks in the supply chain, especially related to hardware manufacturing

5G rollout increases demand for specific minerals that could be sourced from conflict-affected and high-risk areas

Table 7: Impacts in supply chain

Labor rights risks in the supply chain, especially related to hardware manufacturing	
What is the impact?	Risks related to labor rights, working conditions, bonded labor and exploitation of migrant workers in factories are present in Ericsson's supply chain. This is not unique to 5G, but the rollout of new technology requires new equipment to be built and may involve risks for workers, especially when there are short delivery times and other pressures that may increase risks for workers.
Why is it severe?	Throughout the supply chains there are likely to be a vast number of workers, and possibly people in communities, who could be affected. Also, impacts on health, livelihoods and discrimination, among others, can have grave consequences for the individuals concerned.
How is Ericsson involved with the impact?	Ericsson has thousands of first tier suppliers in many countries where social protections and working conditions are limited or even poor. Those suppliers may also have supply chains where labor rights and other human rights are at risk. Depending on Ericsson's actions and due diligence process, it may be contributing to or directly linked to the impacts.
What is Ericsson's responsibility?	Wherever there is a connection between Ericsson's products, services and activities, and potential or actual human rights impacts, Ericsson has a responsibility to identify risks and take action to prevent and mitigate the harm. The UN Guiding Principles give direction on how to prioritize among the many potential supplier relationships and impacts and take targeted and reasonable action to contribute to preventing and mitigating impacts in the supply chain. Such actions can include social audits, but also a focus on training and capacity building in the supply chain, joint action with peers, suppliers and trade unions and addressing root causes, for example by engaging governments where that might contribute to solving systemic issues. Ericsson should also consider its own buying practices, including prices paid and payment terms, and whether these enable suppliers to respect human rights. Where Ericsson has identified that through its own actions or omissions, it has contributed to human rights impacts by a supplier, it should contribute to providing remedy in an appropriate form.

Labor rights risks in the supply chain, especially related to hardware manufacturing

What actions is Ericsson taking, and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson has an established Responsible Sourcing Program to continuously identify and mitigate human rights risks in its supply chain. For more information on the Responsible Sourcing Program click here. Several steps are currently being taken to improve the Responsible Sourcing Program, including updating its audit procedures and implementing a responsible sourcing tool, which will improve the management and dialogue with suppliers. • Ericsson has for a number of years identified labor rights in its supply chain as one of its salient risk areas. In 2020, it conducted a more detailed analysis of which specific human rights are at risk in its supply chain. For more information on the process and the salient human rights risks click here. • A next step in proactively mitigating and addressing these risks is to develop an action plan with concrete actions and initiatives. Such actions are planned to go beyond traditional social auditing, as well as further upstream in its supply chain, where many of the identified risks are more severe. • Ericsson sources a significant number of products and services from a limited number of countries. For these countries, Ericsson should consider carrying out more detailed analysis on the degree to which laws and regulations are aligned with international human rights standards and where some of the risk areas are in its sector. This could then provide the basis to develop guidance for the sourcing organization and suppliers to identify, prevent and mitigate risks in the supply chains in those countries. • Particular attention should lie with Ericsson's own practices and how these could contribute to and potentially exacerbate human rights impacts, for instance due to short delivery times or other pressures on suppliers. The COVID-19 crisis has demonstrated that suppliers can quickly run into liquidity problems if their buyers delay payments, exposing their workers to severe vulnerabilities. Ericsson has seen limited impacts on its supply chain due to the COVID-19 pandemic and has therefore been able to uphold orders made and supply. However, it is monitoring the situations closely and has communicated to suppliers how human rights might be impacted during the pandemic and what steps suppliers are required to take to mitigate such risks. Suppliers are also encouraged to raise any issues with Ericsson in order to find joint ways of addressing them. • Ericsson has conducted specific human rights training for the wider sourcing organization and included this training as mandatory for all supplier-facing job roles. This training is continuously evaluated, and updated when needed, to make sure the sourcing organization stays up-to-date with recent developments and emerging risks.

Table 8: Minerals from conflict-affected and high-risk areas

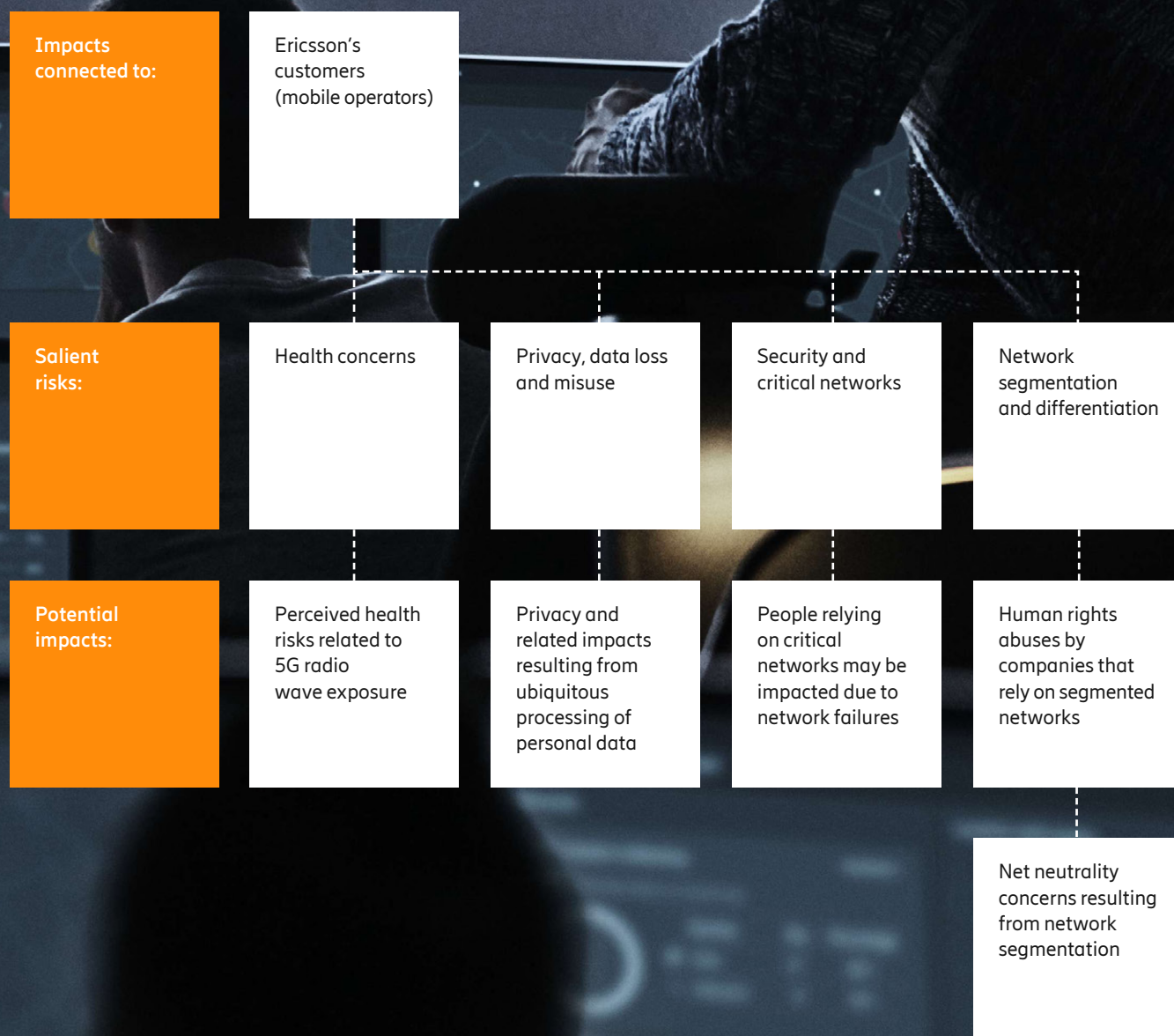| 5G rollout increases demand for specific minerals that could be sourced from conflict-affected and high-risk areas	
What is the impact?	Many Ericsson products, as with electronics in general, require minerals and metals to function. It is well known that these minerals and metals are often mined in conflict-affected or other high-risk areas (for example as a result of weak or non-existent rule of law, presence of migrant workers or child labor) where severe human rights violations linked to the extraction can be found. 5G products will to a large extent rely on the same minerals and metals. However, there is an increased demand specifically for cobalt, copper, nickel and aluminum, primarily used in lithium batteries.
Why is it severe?	Human rights impacts related to conflict and other high-risk contexts are often among the most egregious and severe, including loss of life, forced labor, child labor, gender-based violence, environmental and water impacts on communities, impacts on indigenous peoples, human rights defenders and other minorities and vulnerable groups.
How is Ericsson involved with the impact?	If Ericsson's radio equipment, batteries and other products contain minerals that originate from conflict-affected and/or other high-risk contexts for human rights, and 5G rollout increases demand for such minerals, then human rights impacts associated with the conflict would be directly linked to the 5G equipment. As such, Ericsson has a responsibility to seek to prevent and address these impacts by using its leverage over supply chain actors further upstream. If Ericsson consistently and knowingly uses conflict minerals (or minerals that have other human rights impacts) while failing to conduct adequate due diligence, it may over time be seen to be contributing to such impacts.
What is Ericsson's responsibility?	To address risks related to sourcing of raw materials, Ericsson has a responsibility to ensure that it has effective policies and processes in place that are aligned with the UN Guiding Principles and the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas. In relation to the rollout of 5G specifically, Ericsson has a responsibility to fully map the supply chains of minerals and metals where there is an increased demand and ensure these are sourced responsibly. Where needed, it should also work collaboratively to increase leverage and reach scale in its supply chains.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson already has a program on sourcing of minerals from conflict-affected and high-risk areas. This program is currently being expanded to include additional minerals. For more information click here and here. • Conflict-related impact is one of Ericsson's salient human rights risk areas in its supply chain. It is currently working on developing action plans to address each of the salient human rights risk areas. Since the rollout of 5G will increase the demand for specific minerals, Ericsson will focus efforts on mapping those supply chains. As an example, Ericsson is currently in dialogue with other large Swedish companies in order to work more proactively on the ground in the Democratic Republic of Congo in relation to cobalt mining. Learnings and results from this project will hopefully be scalable to other countries and supply chains of other minerals.

Ericsson's customers (mobile operators)

Impacts connected to:	Ericsson's customers (mobile operators)			
Salient risks:	Health concerns	Privacy, data loss and misuse	Security and critical networks	Network segmentation and differentiation
Potential impacts:	Perceived health risks related to 5G radio wave exposure	Privacy and related impacts resulting from ubiquitous processing of personal data	People relying on critical networks may be impacted due to network failures	Human rights abuses by companies that rely on segmented networks
				Net neutrality concerns resulting from network segmentation

Table 9: Health concerns

Perceived health risks related to 5G radio wave exposure	
What is the impact?	Health concerns are often related to an incorrect perception that 5G will lead to higher radio wave exposure levels, due to technology such as advanced beam steering or higher frequency bands. As with previous mobile networks, 5G devices will communicate with base stations by transmitting and receiving radio waves, or RF EMF. As with the rollout of previous generations of mobile networks, some concerns are raised about possible health impacts from the radio waves related to 5G. Campaigns and protests against 5G have been held in several countries around the world, organized by groups claiming that 5G is not safe. Misinformation and disinformation are also being spread on the internet and social media about 5G health impacts. For example, the early stage of the COVID-19 pandemic led to vandalism of base station sites and threats and harassment towards telecom workers in several countries, as a result of false conspiracy theories claiming that the virus is spread by 5G radio signals, or that these have a negative impact on the immune system. While Ericsson, the wireless industry, expert bodies such as the World Health Organization (WHO) and governments are confident, based on extensive research, that there is no established link between adverse health effects and radio waves from mobile communication equipment, a perception of health risks needs to be addressed. It is important that people have access to fact-based and correct information about 5G and the safety of the technology, so they can formulate an educated opinion. WHO states: "From all evidence accumulated so far, no adverse short- or long-term health effects have been shown to occur from the RF signals produced by base stations" and "A large number of studies have been performed over the last two decades to assess whether mobile phones pose a potential health risk. To date, no adverse health effects have been established as being caused by mobile phone use." (WHO fact sheets No 304 and No 193). Threats and violence directed towards employees in the mobile network industry, as a consequence of the spread of 5G disinformation, are severe human rights impacts that need to be prevented and addressed. Additionally, in cases of base station vandalism, local communities might be impacted as a result of losing access to essential communication services in the area. While the spread of misinformation needs to be prevented and criminal acts never accepted, people have the right to voice concerns.
Why is it severe?	There are no substantiated health effects from radio waves emitted from mobile phones and base stations complying with international science-based limits set with large safety margins. The power levels of the radio signals transmitted by 5G radio equipment are of similar or lower magnitude to those used in previous networks and the same safety standards must be met. While base station site vandalism linked to 5G health concerns is likely to affect a small number of people, any impacts could be grave, for example resulting in impacts for individuals if they temporarily cannot call an ambulance due to the network being unavailable. The health and safety impacts on employees in the mobile network industry as a result of vandalism and threats can also be severe. While potential freedom of expression concerns connected to this impact area have not been substantiated, any such impacts may be severe in repressive countries.
How is Ericsson involved with the impact?	It is typically the responsibility of mobile operators (Ericsson's customers) to comply with national radio wave exposure regulations. However, Ericsson ensures that its radio products are designed and tested to comply with relevant RF EMF standards and regulations. As stated above, there are no substantiated health impacts associated with the radio waves from mobile networks. Issues related to the health and safety of telecom workers, impacts on local communities due to base station vandalism and freedom of expression concerns can be directly linked to business relationships in the value chain. These issues are mainly covered in other impact areas of this report.

Perceived health risks related to 5G radio wave exposure	
What is Ericsson's responsibility?	Ericsson has a responsibility to ensure that its products do not have any adverse health impacts. It does this by complying with safety standards and regulations related to RF electromagnetic field exposure, by making fact-based information about the safety of wireless communications available to stakeholders, and by supporting independent research to address any remaining gaps in knowledge identified by expert organizations such as WHO.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• In accordance with Ericsson's Electromagnetic Fields and Health Policy, Ericsson's radio products are tested in Ericsson's EMF Research Laboratory for compliance with relevant EMF regulations and standards before they are delivered to the market. The EMF Laboratory complies with the international standard ISO/IEC 17025 that specifies general requirements for the competence of testing laboratories and it is accredited by the Swedish accreditation authority SWEDAC. The EMF exposure levels from base stations in places where people normally reside are typically less than a percent of international limits, since the intensity of radio waves drops quickly with distance from the antenna. Base station antennas are installed to ensure that unauthorized people do not have access to areas where EMF limits may be reached. • Ericsson performs research and contributes to international standardization with the aim of developing methods to accurately assess the radio wave exposure from wireless equipment, including 5G. This makes it possible to provide fact-based information to stakeholders. • On its own, and in collaboration with wireless industry associations, Ericsson develops fact-based information about the 5G technology and the radio wave exposure from 5G that is made available to stakeholders. • Additionally, it continuously discusses the topic of 5G, EMF and health with external stakeholders. During the last year, Ericsson participated in more than 30 stakeholder meetings. It will continue to engage proactively and transparently with external stakeholders on this topic to ensure concerns are recognized and addressed. • Ericsson monitors how public sentiment towards 5G and EMF is affected by disinformation, in continuous dialogue with mobile operators and governments, and assists them in efforts to educate concerned citizens. Ericsson will never legitimize vandalism and sabotage of mobile network infrastructure and will always work for the protection and safety of its equipment, workforce, customers and society at large. • For more information on how Ericsson manages radio waves and health click here.

Table 10: Privacy, data loss and misuse

Privacy and related impacts resulting from ubiquitous processing of personal data	
What is the impact?	5G technology is likely to increase the collection of personal data of end users, through the use of connected devices, AI, facial recognition and the availability of more precise geolocation data that is generally used to improve network functionality. Given the increased amounts and types of personal data that will be in circulation as a result of 5G technology, there is potentially an increased risk of adverse impact on the right to privacy if such information is not protected. 5G has enabled an explosion of connected IoT devices and services. IoT devices are generally less secure and new service providers may not always have the necessary controls in place to guarantee the protection of the personal data they handle. These two aspects of 5G are threats to the right to privacy and to Ericsson's principles of personal data protection, in particular its principle of data minimization and transparent and fair processing. Ericsson must consider the changing risk landscape introduced by 5G and implement adequate controls to mitigate these risks.
Why is it severe?	While the potential right to privacy impacts is not necessarily new to 5G, the likelihood of impacts occurring might increase if the risks connected to ubiquitous processing of personal data are not managed correctly. Privacy impacts in and of themselves are grave and for many individuals exposing their private information could lead to serious risks, such as blackmail, leading to impacts on livelihoods and physical threats (for example, because someone's sexual orientation is threatened to be exposed in countries where the law discriminates on this basis), or personal information sold to private businesses (for example, leading insurance companies to deny healthcare coverage, or banking institutions to deny mortgages or personal loans), or the amalgamation of so much information about individuals that the potential for identity theft is significantly heightened (data abuse by governments is discussed in the next section). Many of these impacts are also often hard or impossible to remediate (for example, if someone's sexual orientation is known this cannot become unknown).
How is Ericsson involved with the impact?	If Ericsson was processing data on behalf of a mobile operator or other business partner, and was responsible for loss of or misusing that data, then it would be causing these impacts. However, it is the operators who collect the data. Ericsson could be directly linked to potential impacts related to data loss or misuse through customer or third-party actions, if such impacts are connected to Ericsson services. If Ericsson neglects its responsibility to conduct due diligence into how such services or solutions can be misused, it can be seen to be contributing to impacts caused by third parties.
What is Ericsson's responsibility?	Ericsson has a responsibility to protect personal data in all its operations. It does this by applying strict requirements, design rules, processes, policies and standards and by continuously evolving these practices. Ericsson also has a responsibility to conduct due diligence when engaging with third parties to ensure its products or service offerings are not misused.

Privacy and related impacts resulting from ubiquitous processing of personal data

What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson has a longstanding approach to cybersecurity and privacy, the success of which is central to its business model and proposition. Nevertheless, ICT is a rapidly evolving industry and Ericsson needs to maintain a strong focus on these issues and the evolving risk landscape, including ubiquitous processing of personal data.
	• Building a secure 5G network requires a holistic approach rather than a focus on individual technical parts in isolation. For example, interactions between user authentication, traffic encryption, mobility, overload situations and network resilience aspects need to be considered together.
	• 5G marks the beginning of a new era of network security with the introduction of International Mobile Subscriber Identity (IMSI) encryption. All traffic data which is sent over a 5G radio network is encrypted, integrity protected and subject to mutual authentication (device to network). IMSI is a unique identifiable number stored on each SIM card for mobile phones.
	• For more information on how cybersecurity is built in and ensured in 5G networks click here.
	• There are four main areas that address the different aspects of privacy:
	  • Privacy in product development: Ericsson incorporates privacy by design and all its products are categorized based on their privacy risk profile.
	  • Privacy in deployment and operations: Ericsson only deploys products after they have undergone a privacy assessment.
	  • Standardization of privacy features: Ericsson drives privacy features in multiple standardization organizations, where operators, vendors and other stakeholders set standards for how networks around the globe will work together. This also includes how best to protect networks and users against malicious actors.
	  • Research and horizon: Ericsson conducts research, prepares insights and monitors regulatory impacts to drive a proactive agenda on privacy by design.
	• For many years Ericsson has worked systematically to incorporate privacy considerations into all phases of product development using its internal framework, the Security Reliability Model (SRM). Through the model, it manages risks when developing software and hardware technologies and ensures compliance to regulatory demands such as GDPR. Ericsson is present in all the major standardization organizations working for security and privacy in mobile communication networks. A few of these are mentioned on page 13. It continuously shapes the industry by driving standardization of privacy-enhancing technologies, striving for globally agreed solutions in the mobile networks. For example, Ericsson was one of the main advocates and drivers in 3GPP for protecting 5G against IMSI catchers — a telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users, essentially a "fake" cell tower acting between the target mobile phone and the service provider's real towers.
	• Ericsson also considers privacy risks through its Sensitive Business framework, which evaluates human rights risks in its sales opportunities. While no specific new privacy risks are foreseen related to 5G, existing risks can be heightened. Ericsson continues to monitor such risks and acts proactively when needed. Actions can take the form of developing new use cases and conditions for approval of business opportunities, re-evaluating product risks and implementing new mitigations, as well as raising issues with business partners and external stakeholders.
	• Ericsson has an important role to play in relation to mobile operators, to ensure that the potential for misuse of the technology is minimized. With some operators this will be fairly easy, as they share the same commitments and values as Ericsson. With others it will be much more difficult and a more step-by-step approach will be needed. It will be important to refine and evolve a differentiated strategy to address the diversity that its customers hold in terms of values and commitment to the protection of personal data. Such a strategy also needs to include awareness raising and capacity building.
	• More generally, Ericsson should continue working with mobile operators, peers, other business partners, governments and NGOs to develop strategies to prevent data losses and abuses related to rollout of 5G.

Table 11: Security and critical networks

People relying on critical networks may be impacted due to network failures	
What is the impact?	5G is expected to play a crucial role in facilitating critical infrastructure (such as water and power utilities), health systems (remote surgery, ambulances, home monitoring devices), security provision (police, military) and economic activity. Where these services and their beneficiaries rely on 5G networks and they would fail (including as a result of a cyber attack) people may be severely impacted.
Why is it severe?	Because of the critical nature of the services, impacts could be grave where it concerns life, health and security. In addition, livelihoods may be at stake where critical infrastructure fails for a longer period of time and insecurity is introduced into otherwise reliable systems. The potential to impact vast amounts of people through networks makes the scope potentially large — even where the likelihood (of say a power failure) would be small, this still poses severe risks to people's rights that need to be carefully managed.
How is Ericsson involved with the impact?	Ericsson designs and delivers the networks and, in some cases, manages the networks. While failures of critical networks due to cyber attacks are caused by a third party, Ericsson's involvement will depend, among other factors, on the robustness of measures taken to prevent such attacks. If such measures are robust and in line with industry best practice and impacts nevertheless happen, Ericsson may be seen to be directly linked to potential impacts (rather than contributing to such impacts).
What is Ericsson's responsibility?	Ericsson has a responsibility to proactively identify risks to critical networks, mitigate risks where possible and work with its business partners to inform those most at risk. Where rollout of 5G increases those risks or their exposure, especially where Ericsson is actively developing and promoting new products and functionalities that come with increased risks, then Ericsson should take additional steps to inform potentially affected stakeholders and work with its customers to prevent and mitigate risks to the greatest extent possible, with a specific focus on those people who would be most vulnerable to network failures. It is important to note that cybersecurity is a topic that requires engagement from a wide range of industry stakeholders. Ensuring network security is a combined effort through security standardizations, vendor security processes and operational security, which is the responsibility of mobile operators. Mobile networks often have a multi-vendor setup, meaning that a network consists of products from different vendors. Ericsson needs to take responsibility for its products, services and operations. However, network failures can happen due to circumstances beyond Ericsson's responsibility. External factors such as earthquakes or power outages can also cause network failures, not only deliberate attacks. These risks also need to be addressed.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson proactively identifies vulnerabilities, clearly communicates them to its customers and works together with customers to mitigate any unacceptable risks. • Ericsson's SRM addresses security and privacy risks across its portfolio, including the whole life cycle and end-to-end from sourcing to support. • In addition to Ericsson SRM and connected processes, Ericsson has a dedicated Product Security Incident Response Team, which makes sure that it is effectively able to respond and support customers in case of security incidents involving Ericsson's portfolio. Ericsson PSIRT constantly monitors the security landscape and takes both proactive and reactive measures when necessary. • Ericsson actively contributes to building knowledge and raising awareness on the topic of security of mobile networks by publishing white papers and articles and engaging in the development of standards and frameworks, for example the European Union Agency for Cybersecurity (ENISA) 5G Security Toolbox. • For more information on how Ericsson proactively identifies vulnerabilities click here.

Table 12: Network segmentation and differentiation

Human rights abuses by companies that rely on private networks to operate	
What is the impact?	Through network slicing, 5G will to a larger extent enable companies to have their own private network to run and operate their businesses. Indeed, networks are already being built to support mining operations and automotive manufacturing, among other industries. 5G, often combined with other technologies such as AI, becomes a more integral part of running such businesses, which makes the networks more closely linked to potential adverse impacts that these business relationships may be involved with. This could involve a range of impacts, for example workers being laid off because robots replace their work, enabling automated vehicles that can cause safety accidents, or sophisticated security technology (supported by 5G) that could come with risks for workers and nearby communities. A subset of issues could arise in relation to features of a private network, such as whether it could be used to hide criminal and human rights abusing activity, or, conversely, that certain capabilities of monitoring and content control (by employers) might infringe on privacy rights or freedom of information and expression rights of employees.
Why is it severe?	Not all of the impacts to which Ericsson and its mobile operator customers could be connected to via businesses running private networks will necessarily become severe. However, there could be cases where grave human rights impacts are facilitated by private networks, for example in the case of security operations, or the impacts a mining operation has on local communities. While initially the rollout of private networks through 5G may be limited, over time this could become a significant part of the business, for example when many companies would have their own private network. Thus, this may also become a severe human rights risk due to the number of people that could potentially be affected.
How is Ericsson involved with the impact?	The connection to Ericsson depends on the extent the setup and support of a private network is directly linked to specific adverse human rights impacts. Simply providing services to a business entity that is involved in adverse impacts does not necessarily result in a situation where Ericsson's services are linked to those impacts. However, if the private network facilitates such impacts — for example, impacts on communities by mining companies using specific 5G functionality or accidents with self-driving cars that use a 5G network to navigate the road — then Ericsson's services would be involved with the impact (either through contribution or linkage). Where functionality of private networks goes beyond general communications and instead provides a functionality that specifically leads to a human rights harm and adequate due diligence is not conducted, Ericsson's products and services could be seen to be contributing to such impacts. Ericsson's approach to these types of business engagements is to work together with mobile operators to market and roll out its products and services, as well as prevent and mitigate any adverse impacts. It will be Ericsson's products and services that provide the technology, and, in some instances, Ericsson might manage the networks on behalf of the operator. There is therefore a clear connection to Ericsson's operations. Additionally, many of the same questions that arise in relation to governments' access to and surveillance of networks (see following section) are likely to come up in relation to this business area.

Human rights abuses by companies that rely on private networks to operate	
What is Ericsson's responsibility?	While the challenges laid out here are not unique to 5G, the expected application of network slicing enhanced by 5G will allow more targeted and specific product and service offerings to companies. This requires Ericsson and its mobile operator partners to conduct much of the same type of due diligence process as is in place for other customers, including assessing sales transactions for the potential of human rights abuses and the need to build and apply leverage in relation to these companies, together with the mobile operator and other parties, in order to prevent and address human rights abuses connected to the segmented networks.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• To some extent these risks are identified and addressed through the Ericsson Sensitive Business framework. However, there is a need to expand this approach to ensure risks are captured proactively and consistently, given that the rollout of 5G will likely increase the offering of private networks. • There could be a need for additional sector-specific risk analysis and guidelines for sectors where these setups will be rolled out first — likely healthcare, retail, automotive, smart manufacturing and mining. Where possible, such analysis could be done in collaboration with mobile operators. • Furthermore, specific privacy and freedom of expression risks in relation to corporate networks (intranets) need to be considered and incorporated in design, sales and rollout of such private networks.

Table 13: Network segmentation and differentiation

Net neutrality concerns resulting from network segmentation	
What is the impact?	Net neutrality is the principle that all users have the same right to access and distribute information, and run services and applications of their choosing, on the internet. 5G is designed to increase and improve communication capabilities for a wide range of different uses, each with their own network capacity requirements. Mission-critical real-time services, such as road safety applications, demand one type of network characteristic. Massive IoT services, connecting large numbers of devices for services that are not time critical, demand another. Network slicing is a way of creating different "virtual networks" using the same infrastructure, which allows these virtual networks to be tailored to their services' capacity needs and adjusted according to user/traffic demand. While network slicing is not a new feature, its use will increase in 5G networks. Such functionality alone does not impact net neutrality, but it is possible to misuse the technology for other purposes.
Why is it severe?	The concerns related to net neutrality are that the increased possibilities of network slicing in 5G networks can be used to differentiate offerings in a way that severely impacts the ability of users to fully utilize certain services. This can include hampering their ability to access online education platforms, basic and/or critical information and services (such as doctor appointments), or effectively do their job remotely. The importance of these scenarios has been brought sharply into focus during 2020 with the COVID-19 pandemic. Human rights, such as the rights to education, health, non-discrimination, just and favorable conditions of work and an adequate standard of living, could be harmed in these circumstances.
How is Ericsson involved with the impact?	Where Ericsson provides networks with segmentation capability that is misused in a way that impacts people, its products and services could be linked to the human rights impacts previously outlined. The nature of the company's involvement changes in the event that Ericsson does not take action to minimize impacts or influence the extent to which network segmentation by a customer could lead to a poor quality of network or inability to access the internet by some end users.
What is Ericsson's responsibility?	Given that net neutrality and how it impacts human rights is a complex dynamic and may vary considerably depending on context, it is important that Ericsson engages with relevant stakeholders to ensure the principles of net neutrality (the equal access to information and services) are protected through effective legislation. Ericsson also has a responsibility to ensure its products and solutions are not misused and to use its leverage with customers to prevent harm.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson supports an open internet that allows end users to access the content, applications and services they want, while enabling continued investment, customization and innovation in the services they need. It does this by engaging in the development of regulatory requirements to protect equal access for end users; for example, the EU Open Internet Regulation. It is important to note that regulation protecting net neutrality should focus on ensuring that all users get equal access to content and services, but avoid provisions requiring that all individual packets of data must be treated the same. Such requirements would prevent some of the crucial functionality of 5G networks, such as tailoring the network specifications so that each service can get a virtual network to suit its individual needs. For example, a mobile network on a train needs to manage sophisticated cybersecurity protections and allow travelers to stream video. Network slicing ensures that these functionalities can be managed effectively through the same network. • Ericsson will continue to engage on this topic to promote and develop effective legal standards to ensure equal access to information, services and applications. It believes the EU, through the Open Internet Regulation, has taken the right approach to address this issue. • Ericsson is additionally engaged in standardization bodies where network slicing is defined. The aim is to achieve a transparent definition of slicing technology, which guarantees harmonization and global alignment of technology standards and industry initiatives. This in turn facilitates a better understanding of the technology among regulators, ensuring concerns are addressed and rights protected through effective legislation.

Ericsson's involvement with governments

Impacts connected to:	Ericsson's involvement with governments		
Salient risks:	Network surveillance	Network shutdowns	Network segmentation and differentiation
Potential impacts:	Government surveillance and extraction of information by authorities for harmful purposes	Network shutdowns targeting specific groups of people or institutions	Government authorities using networks to facilitate human rights abuses

Table 14: Network surveillance

Government surveillance and extraction of information by authorities for harmful purposes	
What is the impact?	As discussed earlier in this report, and spurred by 5G technology, companies will increasingly generate a huge amount of personal identifiable information, which government authorities might want to access. 5G is also likely over time to enable more precise surveillance by processing larger amounts and new types of data sets. While such efforts by many governments may be developed in the context of legitimate purposes such as crime prevention, emergency response and countering terrorism, the existence of such vast amounts of data makes it prone to abuse. This would impact the right to privacy and, depending on the context in which that right is violated, other impacts such as discrimination, arbitrary arrest, infringements on free press, organization, elections and so on.
Why is it severe?	While these risks are not new to 5G, the vast amounts of user data that will further exponentially increase with the rollout of 5G is likely to create substantial privacy, and other related risks, for large numbers of people. This is a particular concern in countries with repressive and authoritarian regimes, or where there are weak privacy laws and/or enforcement of such laws.
How is Ericsson involved with the impact?	Networks provided by Ericsson contain and will contain personal identifiable information that authorities may wish to access. For example, location capabilities and call logs are basic functionalities and information in mobile networks that enable communication in the first place. Being able to locate devices is necessary in order to connect calls and optimize network performance, while call logs are used for charging and billing. Through the provision of network products and services, Ericsson enables users to channel private information over networks that could then be captured by government entities interested in that private information. Ericsson does not develop surveillance technology. However, it does enable lawful interception (LI) functionality in its networks. LI is a regulatory requirement in virtually every jurisdiction. A mobile operator must have an LI function in the network to be allowed to run a public telecom network. For Ericsson this means that if it cannot provide LI functionality, it is disqualified as a supplier of network equipment.

The European Telecommunications Standards Institute (ETSI) specifies a reference architecture and the information that should be intercepted and supplied to a law enforcement agency. Ericsson's implementation of the ETSI specification consists of 1. Interception Management System LI-IMS and 2. LI functionality in network elements. The LI-IMS is the gateway between the operator and agency domains and implements the LI administration function and the mediation functions. Ericsson only provides products for the operator, not the state authority or agencies such as monitoring centers.

While Ericsson, as a vendor, does not interact directly with government authorities requesting this type of information (such requests are directed to mobile operators), the gathering and sharing of such information is nevertheless enabled through functionalities in the network itself. Ericsson also in some cases manages networks for mobile operator customers. In these cases, it is still the mobile operator that receives the actual request from the government. Ericsson will then execute the request based on information provided by the mobile operator. Ericsson could potentially contribute, or be directly linked to, impacts as a result of misuse of its technology, which will in part depend on the quality of due diligence measures taken to identify and mitigate such risks.

Additionally, in many countries, governments have the capability to directly access networks and extract information without the knowledge of either the operator or Ericsson. In these scenarios Ericsson could be directly linked to such impacts, and where it does not take reasonable steps to mitigate against the risks, it could also be seen to be contributing. |

Government surveillance and extraction of information by authorities for harmful purposes	
What is Ericsson's responsibility?	Given the variety of ways in which Ericsson could be connected to these impacts, it has a responsibility to consider the various scenarios and the type of responses that would be needed to prevent and mitigate human rights risks. It should also consider potentially vulnerable groups such as journalists, human rights defenders, political opponents and ethnic minorities, that might be specifically targeted by government surveillance efforts. 1. Ericsson has a responsibility to consider what it can do in product design and delivery to avoid misuse of data extraction capabilities and consider the extent to which 5G makes it more (or less) likely that this would occur. 2. Ericsson has a responsibility to consider how it can avoid third parties, including governments, gaining access and extracting data from end users, including through hacking and wiretapping. 3. Where Ericsson is involved in the activity, potentially infringing on privacy and other rights (for instance when managing networks for customers and requests from a mobile operator), it has a responsibility to have clear conditions and guidance for when such activity may take place, and escalation pathways for its employees (and contract workers conducting the same activities) when such requests are made, including due consideration for the safety and security of all staff. 4. Where customers or other third parties receive government requests or orders for extraction and sharing of private data, Ericsson has a responsibility to consider the risk of abuse in the sales process and implement safeguards to minimize human rights impacts and exert leverage, including contractual agreements, capacity building and influencing government policy to incorporate respect for human rights.

Government surveillance and extraction of information by authorities for harmful purposes	
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• As mentioned under impact areas in the "What is 5G?" section (page 39), Ericsson has well-established processes to build in privacy by design in product development. Product risks are also evaluated through the Sensitive Business process. • See the "What is 5G?" section (page 40) on how Ericsson is managing cybersecurity risks in its networks and in the rollout of 5G. • Ericsson's Sensitive Business framework specifically considers risks to privacy and freedom of expression in relation to sales engagements, including where data misuse may be a risk. The process aims to ensure that business opportunities and engagements are conducted in accordance with international human rights standards. When risks are identified in a sales opportunity through the process, the Market Area must submit an approval request. Submissions are evaluated according to four risk parameters (product risk, country risk, customer risk and purpose risk) and may be approved, approved with conditions or rejected. Conditional approvals include technical and/or contractual mitigations and its implementation is monitored to ensure adherence. • In relation to government surveillance and privacy, Ericsson has developed approved use cases and end-user agreements that are contractually binding, specifying for what purpose the customer is allowed to access certain personally identifiable information. Any actions outside of the approved use cases constitute a breach of contract. With the deployment of 5G, new use cases might need to be developed. A process to identify potential gaps or additional requirements has been initiated. The current use cases applied by Ericsson have developed over time, based on learnings from previous engagements and internal evaluations. Additionally, the effectiveness of potentially new 5G use cases will take time to fully evaluate. • Ericsson only supplies LI interfaces that are approved by international standards. In order to mitigate misuse of this technology, access to the LI system is controlled by multi-factor authentication, login credentials and certificates. Data integrity and completeness is secured by encryption and digitally signed data. All activities in the LI system are also logged to ensure traceability and accountability. When there is an alleged misuse case such record-keeping can prove how the LI system was used and for what purpose. Furthermore, the LI solution is designed to intercept a fraction of the users and traffic in the network, effectively preventing mass surveillance. • Ericsson is continuously evaluating its procedures relating to LI, including when it manages a network on behalf of a mobile operator, to further strengthen the safeguards protecting against intended misuse of LI functionality. • Where governments have direct access to networks (this can be done in many different ways, for example probes installed in the network, physical routing of cables through government facilities, or mandating that mobile operators accept government officials' access to certain facilities and computer programs, so they can monitor and/or extract user data at will) it is challenging for mobile operators or vendors to prevent such access because the companies are taken out of the loop. Information on direct access capabilities of governments is also not usually easily accessible, because it is a question tied to national security. Laws enabling such government access are often vague or overly broad. • As a member of the Global Network Initiative, a multi-stakeholder initiative promoting the right to privacy and freedom of expression in the ICT industry, Ericsson has a collective role to play in raising awareness about direct access setups and laws that enable governments to access networks directly. Governments have a duty to make sure safeguards and access to effective remedy are implemented and accessible to users. The industry can use its collective leverage to influence governments to implement such safeguards. Currently Ericsson is working with other GNI members to better understand direct access setups and how human rights can be protected. • Ericsson has also initiated dialogue with civil society organizations on potential collaboration to raise awareness on technology misuse among human rights defenders.

Table 15: Network shutdowns

Network shutdowns targeting specific groups of people or institutions	
What is the impact?	The possibility of shutting down a network is not new to 5G. But, as the networks become more sophisticated, and through the proliferation of private networks, there is potential for more discrete and granular ways to shut down parts of networks (or lower data transmission speeds), enabling governments to target specific groups, for example: • a geographic location with an ethnic minority or where many of the governments' opponents are based • shutting down specific buildings (such as those of the opposition party) • cutting off or slowing down the network for citizens, while private government and company networks continue operating As communities and societies increasingly rely on mobile networks for critical services (such as first responder services and utilities) this could provide repressive governments with a very powerful tool to suppress opposition and manipulate populations.
Why is it severe?	Network shutdowns could potentially affect large groups of people and lead to grave impacts, such as infringements on the rights to freedom of expression and organization, privacy, access to essential services (and therefore life, health, security and livelihoods), non-discrimination and indigenous communities' rights. Additionally, if protests against new technology take place in countries with repressive regimes, there is a potential risk of suppression, which may result in impacts on the right to freedom of expression.
How is Ericsson involved with the impact?	All networks, including those provided by Ericsson, commonly have a feature to shut them down, and there is no specific technology involved in enabling a shutdown. Shutdowns can in some cases be necessary for public safety reasons, for example preventing crimes or terrorist attacks. Government requests to shut down a network are directed at mobile operators. Ericsson is therefore generally directly linked to potential impacts as a result of a shutdown. When Ericsson is providing Managed Services to customers it is still the mobile operator who receives the request from the government, but this request is then acted upon by Ericsson personnel. In such situations Ericsson might be contributing if it has no systems in place to check and question the request, and it did not raise the issue with the mobile operator in contract negotiations. Of course, mobile operators and governments are also likely to be contributing to impacts in such cases.
What is Ericsson's responsibility?	Ericsson has a responsibility to consider these risks in the design and rollout of the networks and prevent and mitigate impacts. In particular, it needs to be attentive to whom and how it markets network segmentation and targeted shutdowns as a useful product feature for governments to adopt as part of the 5G rollout. Where its own staff may be at risk of receiving requests to shut down networks, as part of a managed services agreement, Ericsson has a responsibility to ensure that all requests are legitimate and ensure the service provider can provide the proper documentation from government authorities to demonstrate that all legally required procedures have been followed. In cases when requests are not legitimate, Ericsson has a responsibility to raise the issue with the customer and build leverage into contracts to be able to do so.

Network shutdowns targeting specific groups of people or institutions

| What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact? | The potentially more discrete and granular capabilities of shutting down mobile networks as a result of more sophisticated 5G technology needs to be closely monitored. It is still too early to say to what extent this risk will materialize. However, Ericsson will ensure these issues are included in its due diligence processes and proactively engage with mobile operators to discuss how this risk could materialize based on their experiences, in order to find joint ways of approaching this risk.

Ericsson is continuously evaluating its procedures relating to how it manages a network on behalf of a mobile operator, to further strengthen the safeguards protecting against intended or unexpected impacts connected to network shutdowns.

If protests relating to new technology, linked to Ericsson, do emerge in repressive countries, Ericsson needs to be aware of the situation and address it through due diligence measures. It should work in collaboration with mobile operators and other partners and stakeholders to build leverage with governments and engage them on approaches to obtain buy-in from citizens.

The GNI is actively engaged in raising awareness on government-mandated shutdowns globally and advocating for lifting such shutdowns when they are clearly in violation of human rights. To increase collective leverage, Ericsson will continue to engage on this issue through the GNI and gather information in order to more clearly understand if and how 5G technologies will provide governments with more sophisticated tools to shut down networks. |

Table 16: Network segmentation and differentiation

Government authorities using private networks to facilitate human rights abuses	
What is the impact?	As is the case with private enterprises, government authorities are increasingly using private mission-critical networks for internal communications. It could be a dedicated network for emergency response services, but also a police department or security services which may be involved in human rights abuses organized through network communications, such as by coordinating operations. Additionally, military actors are increasingly looking to utilize 5G technology (and coming generations) for a wide range of use cases.
Why is it severe?	Human rights abuses relating to police and security services are often of a grave and irremediable nature such as loss of life or severe injuries. Many other severe impacts may be involved, as well as loss of livelihoods, gender-related violence and impacts on children and other vulnerable individuals.
How is Ericsson involved with the impact?	Ericsson's connection to potential abuse perpetrated by government authorities through private networks will largely depend on the extent to which the abuse was enabled through the use of the network and the due diligence measure it took in order to mitigate risks of such impacts. 5G will likely make private networks and services more widespread among governments. Ericsson's approach to these types of business engagements is to work together with mobile operators, not supplying government entities directly. Challenging scenarios are also likely to occur, such as where Ericsson may be involved in providing network services for emergency response services, including police authorities. While mobile communication and connectivity is a crucial part of providing emergency response services, police forces can also be involved in human rights abuse.
What is Ericsson's responsibility?	Ericsson has a responsibility to ensure its networks are not used to facilitate human rights abuse. The fact that it supplies government entities through a mobile operator customer does not diminish that responsibility. Ericsson needs to identify, prevent and mitigate risks related to such government customers. As Ericsson further assesses its responsibility under the UN Guiding Principles for specific transactions and relationships, it will seek clarity on its responsibilities and the type of action it can and should take.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• To date, the Ericsson Sensitive Business framework has primarily focused on freedom of expression and privacy risks. However, Ericsson is in the process of evaluating how broader human rights risks in relation to government end users should be addressed. It already considers the human rights track record of government customers and will formalize this approach. • Ericsson is also in the process of including a conflict sensitivity perspective in its sales process, to proactively identify business engagements in conflict-affected areas and implement appropriate mitigating measures. • In collaboration with mobile operator customers, Ericsson is also developing offerings that take into consideration ways in which its products and services might facilitate human rights abuse by government end users, and work with mobile operators to develop joint tools to prevent and mitigate these risks.

Ericsson's broader societal impacts

Impacts connected to:	Broader society	
Salient risks:	Societal impacts	Trustworthy AI
Potential impacts:	5G technology could contribute to socio-economic inequality between and within countries	Ethical challenges presented by AI and machine learning, specifically with respect to trustworthiness, human oversight, bias and transparency

Table 17: Socio-economic inequality

5G technology could contribute to socio-economic inequality between and within countries	
What is the impact?	A digital divide already exists, with more than 40 percent of the world's population lacking internet access. While Ericsson forecasts that 90 percent of the global population will be covered by 4G networks by 2026, the same estimate for 5G is 40 percent by 2026.[11] The COVID-19 pandemic clearly shows that inequalities in access to connectivity affect access to education, healthcare and livelihoods. There is also evidence that mobile broadband penetration contributes to Gross Domestic Product (GDP) growth. A joint research project between Ericsson and Imperial College in London shows that, on average, a 10 percent increase in the mobile broadband adoption ratio causes a 0.8 percent increase in GDP.[12] 5G is being rolled out with different speeds across regions and within countries. With all of the potential economic, social and cultural benefits 5G will bring, such developments, if rolled out unequally, can also further create and exacerbate inequalities between developed and less developed countries and between urban and rural communities within countries. This can lead to potential impacts on livelihoods and further drive inequalities. Additionally, some governments may use the rollout of 5G as a political tool, benefiting their preferred groups over others.
Why is it severe?	While generally the impacts are quite unpredictable, the issue of digital divides almost by definition affects large groups of people and is therefore potentially widespread. A wide range of human rights (such as rights to health, education and livelihoods) can potentially be affected by an uneven rollout, increasing the scope of the impacts.
How is Ericsson involved with the impact?	Addressing the digital divide and mitigating risks related to an uneven rollout of 5G networks is an issue connected to the whole ICT ecosystem. As a network vendor, Ericsson is closely involved in how networks are rolled out and is one of the main actors in the ecosystem that has a role to play. Ericsson may be inadvertently contributing to this issue if it is not appropriately managed.
What is Ericsson's responsibility?	Ericsson has a responsibility to proactively drive the issue of bridging the digital divide. While it is not its intent to drive impacts relating to creating digital divides, it is connected to the impacts its networks create. Ericsson cannot, however, address these risks on its own, but must work with customers, industry peers and governments to ensure that the ICT industry is conscious of these issues, recognizing them in business strategies and engagement with stakeholders, and identifying any egregious forms, for example when a government is deliberately disadvantaging a particular ethnic minority in rolling out the benefits of 5G. While such forms of deliberate impacts will be difficult to assess, and primarily linked to spectrum allocation and licensing, Ericsson needs to be aware of the risk and continuously engage relevant stakeholders to identify red flags.
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• As previously stated, these types of broader societal impacts (contributing to changing demand for particular types of labor is an additional impact) are not an issue that Ericsson can solve on its own. It has been addressing the issue of digital inclusion for many years through a wide range of programs, collaborations and initiatives. • While improving capacity and extending coverage is a priority, this does not totally address the problem of digital inclusion. The internet must also be accessible, affordable and ready for use by all. Driving digital inclusion goes beyond the provision of network coverage, with accessibility and affordability as key barriers for potential users.

[11] Ericsson Mobility Report (January 2019) and Ericsson Mobility Report (November 2020)
[12] Boosting GDP through mobile broadband

5G technology could contribute to socio-economic inequality between and within countries	
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Through its work in forums such as the Broadband Commission for Sustainable Development, the World Economic Forum, the Alliance for Affordable Internet and the Smart Africa Alliance, Ericsson aims to ensure that the benefits of broadband, which underpin achievement of the Sustainable Development Goals, are affordable and accessible to all. In these forums Ericsson advocates efforts such as spectrum policies and international investments, as well as progress towards connecting the unconnected and exploring multi-stakeholder business initiatives to bridge the digital divide. Ericsson is also engaged in capacity development with partners including the Swedish International Development Cooperation Agency (SIDA) and SPIDER, one of the programs focusing on capacity building so that populations will have access to good quality and secure telephony and broadband services and communications. • Ericsson is relaunching its strategy on Digital Inclusion, involving institutional capacity building, digital literacy and universal and affordable internet access through mobile broadband. A detailed scope, desired outcome and strategy will be developed during 2021. • Connect to Learn is Ericsson's flagship education program. Its purpose is to empower teachers, students and schools through ICT solutions to deliver a quality 21st century education, as well as providing young people worldwide with digital skills to prepare them for a 5G future. • In 2020, Ericsson and UNICEF launched a global partnership to map school internet connectivity. The three-year initiative to identify connectivity gaps in 35 countries is a critical first step in connecting every school to the internet. This joint effort is part of the Giga initiative. Launched last year and led by UNICEF and the ITU, Giga aims to connect every school to the internet. In addition to funding, Ericsson will commit resources for data engineering and data science capacity to accelerate school connectivity mapping. Specifically, Ericsson will assist with the collection, validation, analysis, monitoring and visual representation of real-time school connectivity data. The data generated through the mapping will enable governments and the private sector to design and deploy digital solutions that enable learning for children and young people. Ericsson will also engage its extensive customer base to further advance the goals of the Giga initiative. • Ericsson partners with UNESCO on an AI literacy program, teaching AI skills to children from kindergarten to grade 12. The centerpiece of the solution is the Teaching AI for K-12 portal that is a free resource, accessible globally for teachers and curriculum developers to help them in their efforts to create new learning programs for K-12 students on the subject of AI. In addition, independently from UNESCO, Ericsson provides AI introductory courses targeting children and young adults (11 to 25 years old). It is currently in discussions with universities to develop advanced AI courses for university students. • For more information on Ericsson's efforts to bridge the digital divide and provide connectivity for all, read its Technology for Good Impact Report. • While Ericsson has not seen any examples of governments using the rollout of 5G networks as a political tool, benefiting preferred groups over others, this is an issue that needs to be monitored in close dialogue with its mobile operator customers, to ensure it does not inadvertently contribute to such political agendas. • In relation to 5G specifically, Ericsson needs to ensure it not only considers digital divides between more and less developed countries, but equally considers divides within countries between urban and rural areas — not only focusing on smart cities, but also on clever countrysides (the future connectivity needs of rural areas). Connectivity challenges and needs are very different in urban and rural areas — rather than issues such as smart transportation and parking, in rural areas use cases are about connected farms or remote surgery. The rollout of 5G networks in urban and rural areas must reflect the different needs of such communities. In order to address these needs close collaboration with customers and governments is necessary, as well as active engagement with local communities to ensure their needs and concerns are addressed.

Table 18: Socio-economic inequality

Ethical challenges presented by AI and ML, specifically trustworthiness, human oversight, bias and transparency	
What is the impact?	AI and ML, powered by 5G technology, has in a relatively short space of time successfully automated routine tasks and enabled more efficient networks, while enhancing human capacity with new knowledge. It has the potential to enable greater innovations, that could solve some of the most difficult societal, environmental and economic concerns. As a result, AI is likely to bring about sweeping changes in businesses and in the ways people work and live in the years ahead. The total impact of these changes is still to be discovered, and there is potential risk for intentional adversarial misuse, which Ericsson aims to mitigate as far as possible, through security and privacy design. But previous experiences have revealed that some unforeseen outcomes could also result in negative unintentional side effects. This could include the exposure of users' personal data, unfair judgements through opaque automated decision making, or just the uncertainty of where accountability lies in the event of an autonomous system malfunction. This technological revolution is likely to bring significant people-related disruption in its trail, leading to calls from within and outside the technology community to regulate the development of AI, or at the very least provide a global framework that establishes the key principles of ethical and trustworthy AI.
Why is it severe?	Ericsson mainly develops and uses AI solutions to run more efficient networks. Examples of use cases are AI-powered support services — which can isolate faults more accurately in the 5G network to remedy issues correctly and quickly — or using AI algorithms to predict traffic patterns and autonomously turn off antennas as required to reduce energy usage. While such use cases generally have a positive impact on people and the environment, there needs to be awareness of the impact that AI-enabled systems might have while being implemented in different contexts. AI systems also need to be programmed to act responsibly and fairly within their boundaries for trustworthy outcomes. There are several challenges with the potential of AI technologies and possible unintended effects. These include: • Transparency and explainability: If AI systems are opaque and unable to explain how or why certain results are presented, this lack of transparency will undermine trust in the system. In which ways can autonomous systems explain themselves? • Security and privacy: Access to vast amounts of data will enable AI systems to identify patterns beyond human capabilities. This creates a risk that the privacy of individuals could be breached. There is even the risk that our innermost private thoughts could be accessed and (unknowingly) influenced, potentially impacting people's right to freedom of thought. How can we as individuals secure and comprehend the use of data derived from our activities online or in real life? • Personal and public safety: Deploying autonomous systems (self-driving cars, UAVs or robotics) across public or industrial arenas could pose a risk of harm. How can we ensure human safety? • Bias and discrimination: Even if technology is neutral, it will only do what we program (and teach) it to do. It will therefore be influenced by human and cognitive bias, or skewed, incomplete learning data sets. How do we make sure that the use of AI systems does not discriminate in unintended ways? • Automation and human control: Trust in systems that both support and offload current work tasks have the risk of undermining our knowledge of those skills. This will make it more difficult to judge the correctness and outcome of these systems and, in the end, make it impossible for human interception. How can we ensure human control of AI systems? • Accountability and regulation: With the introduction of new AI-driven systems, expectations on responsibility and accountability will increase. Who is responsible for the use and potential misuse of AI systems?

Ethical challenges presented by AI and ML, specifically trustworthiness, human oversight, bias and transparency	
Why is it severe?	These challenges have the potential to impact large groups of the population through 5G networks, if left unaddressed. Additionally, a wide range of human rights are potentially impacted by intentional or unintentional misuse of AI solutions. Big data analytics and AI increasingly enable states and business enterprises to obtain fine-grained information about people's lives, make inferences about their physical and mental characteristics and create detailed personality profiles. An increasingly complex web of commercial organizations within a broad data ecosystem is collecting this granular information in order to make inferences about what people think, feel, want and ultimately how they will act, in order to monetize this data. One of the main problems with this data collection is that it often happens without the data owner's/rights-holder's knowledge or consent, and thus without any awareness of, or control over, the myriad ways in which their personal data could be used. The number of people potentially impacted by this range of important issues could be extremely high, involving anyone with a technology device.
How is Ericsson involved with the impact?	5G technology provides the infrastructure to generate and transport massive amounts of data. AI provides the tools to make sense of the data, which can be used to reduce the complexity of the system by automation, optimize the network for performance and efficiency and to introduce new business innovations. Ericsson, as a provider of the advanced infrastructure and connected AI solutions, plays a pivotal role, even though most of the potential pitfalls and challenges of using AI are not connected to AI solutions specifically developed for the telecom industry. However, Ericsson could be directly linked to impacts as a result of a wider range of AI solutions deployed in connection to 5G networks; for example, if government authorities use AI solutions in combination with speech recognition to almost instantly process intercepted calls. While Ericsson does not develop this type of AI solution, it needs to consider the risk of enabling such misuse in 5G networks. If Ericsson fails to take sufficient actions to prevent such abuse by third parties, it could be seen to be contributing to the impacts.
What is Ericsson's responsibility?	As one of the key enablers of AI solutions, Ericsson is an important stakeholder in ensuring trustworthiness of AI applications and a key voice to engage with industry peers and governmental stakeholders on this topic. It has a responsibility to consider human rights risks in the design, development, use and sales of AI solutions and exert its leverage to guide discussions towards an enabling environment where risks to people are effectively addressed.

Ethical challenges presented by AI and ML, specifically trustworthiness, human oversight, bias and transparency	
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• Ericsson decided in 2019 not to create yet another set of ethical principles for AI development, but rather work with existing standards. Following this decision, and based on comprehensive analyses of existing standards, it decided to adopt the European Commission Ethics Guidelines for Trustworthy AI and implement these guidelines into Ericsson policies and processes. The EC Guidelines outline seven principles for trustworthy AI: 1. Human agency and oversight: AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop and human-in-command approaches. 2. Technical robustness and safety: AI systems need to be resilient and secure. They need to be safe, ensuring a fallback plan in case something goes wrong, as well as being accurate, reliable and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented. 3. Privacy and data governance: Besides ensuring full respect for privacy and data protection, adequate data governance mechanisms must also be ensured, taking into account the quality and integrity of the data and ensuring legitimized access to data. 4. Transparency: The data, system and AI business models should be transparent. Traceability mechanisms can help achieve this. AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system and must be informed of the system's capabilities and limitations. 5. Diversity, non-discrimination and fairness: Unfair bias must be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life cycle. 6. Societal and environmental wellbeing: AI systems should benefit all human beings, including future generations. It must be ensured that they are sustainable and environmentally friendly. Moreover, they should take into account the environment, including other living beings, and their social and societal impact should be carefully considered. 7. Accountability: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes, plays a key role, especially in critical applications. Adequate and accessible redress should also be ensured. • Ericsson has a good understanding of what challenges it needs to address in order to minimize possible negative effects of its technology. It now needs to create practical ways to implement these findings across relevant functions within the company — a toolkit it can use to operationalize the ethical principles. So far, specific design rules based on the EU AI Guidelines have been developed. • The challenges and risks related to trustworthy AI will most likely be addressed through national or regional legislation and regulations, policy frameworks and/or standardization. Examples of such regulations are already emerging. There is an ongoing discussion with the EU to understand the need to turn part of the EC Guidelines into European-wide policies or regulations in the area. In parallel, standardization bodies such as ITU, IEEE, ETSI, CEN/CENELEC, NIST, SIS and ISO have started working groups to explore the options for standardization.

Ethical challenges presented by AI and ML, specifically trustworthiness, human oversight, bias and transparency	
What actions is Ericsson taking and what additional actions will Ericsson take to prevent and mitigate this impact?	• As with all regulation and standardization efforts, being part of the ongoing process provides a possibility to influence the outcome. Regulations and standards will help the industry to create truly global solutions that adhere to the challenges previously described. However, if they are too rigid, they might create barriers and infuse fear in society that will hinder further innovation and/or positive usage of the technology. Ericsson has a responsibility to push for regulation that has a clear human rights approach and is aligned with other legal developments within responsible business, such as the introduction of mandatory human rights due diligence requirements. • Not all the challenges discussed are topical for the telecom industry, but for those that are, Ericsson needs to conduct risk assessments and ask itself what the impact is if something goes wrong. In addition, it needs to be mindful that depending upon context, some principles may override others, and for various AI use cases, these will apply differently. • There is still a lot to learn in this area. Together with its stakeholders, Ericsson needs to define a set of relevant use cases topical for mobile connectivity to refine requirements and define assessment methodology.

Cross-cutting actions

Key internal frameworks and processes can help centralize and coordinate efforts to address human rights risks. Ericsson's processes include use of the Sensitive Business framework, responsible sourcing and remedy and grievance mechanisms.

Many of the identified impact areas touch upon cross-cutting themes and issues that need a centralized and coordinated effort, rather than just an issue or business area approach. Such cross-cutting attention recognizes the interconnectedness of issues and the need to address them holistically if Ericsson is to effectively take action to prevent and mitigate human rights risks as they relate to 5G. Cross-cutting attention and coordination also emphasizes and facilitates shared responsibility for human rights risks and responding to them. The following are key internal processes and frameworks needed to address these cross-cutting issues.

The Sensitive Business framework
The main framework through which Ericsson manages human rights risks relating to customers and misuse of its technology is the Sensitive Business framework. This due diligence process was one of the first of its kind in the ICT industry when it was developed more than a decade ago and is still a leading process. The framework aims to ensure that business opportunities and engagements are conducted in accordance with international human rights standards.

The Sensitive Business Board, part of the Sensitive Business framework, is a company-wide forum that comprises Ericsson's senior management, oversees the execution of the Sensitive Business framework and meets regularly. When the Sensitive Business automated tool identifies risks in a sales opportunity, the Market Area submits an approval request, which the Sensitive Business unit evaluates according to its business risk methodology (which includes country risk, customer risk, product risk and purpose risk). Cases are approved, approved with conditions or rejected. Conditional approvals include technology and/or contractual mitigations, and its implementation is monitored to ensure adherence.

The Sensitive Business framework is currently undergoing a major transformation. The transformation will, through the introduction of a more automated process, enable Ericsson to focus its resources on more complicated and high-risk cases, while ensuring that a larger number of cases are fully evaluated. In order to further strengthen and align the framework with the UN Guiding Principles, the following additional actions are identified:

- The scope of the evaluated human rights risks needs to be expanded, in order to cover not just the rights to privacy and freedom of expression. While these risks are still identified as the most salient for Ericsson in relation to end use of its technology, additional risks such as conflict-related impacts need to be addressed. Ericsson is currently in the process of expanding the Sensitive Business methodology to ensure a broader set of risks are covered.

- Tracking performance of actions taken and acting on actual impacts is challenging to manage. In order to cover the full scope of human rights due diligence, these challenges need to be addressed. Ericsson is currently exploring ways of including rights to verification of agreed contractual mitigations and use cases. Given that potential misuse of technology is often linked to national security in a specific country, verifying such misuse is difficult. Nevertheless, this is an identified improvement area that it needs to address in order to better react in case misuse is identified.

- Beyond contractual or technical mitigations, or alternatively deciding not to sell to a particular customer (for example because of its track record on human rights), Ericsson is exploring how to expand the measures used to prevent and mitigate risk. This includes building and applying leverage of various kinds, including commercial leverage, other bilateral engagement such as capacity building and awareness raising (for example of customers and civil society organizations) and collaboration with peers to create industry-wide change or engage governments jointly. To some extent these types of actions are pursued through Ericsson's membership in the GNI. However, it is considering how to scale up its approach.

Responsible sourcing
A significant portion of Ericsson's human
rights risks can be found in its supply
chain. This is also true for the rollout of
5G. In order to have a more focused and
proactive approach to addressing human
rights risks in its supply chain, Ericsson
recently conducted a detailed analysis of
its supply chain to define salient human
rights risks.

Ericsson has developed the list of salient
supply chain human rights issues based
on internal and external expertise and
stakeholder consultations, audit results
and comprehensive analysis of its supplier
categories, including factors such as
relevant industry, type of activities, country
of operations and nature of the workforce,
including potential vulnerable groups.[13]

While the full scope of human rights
risks will continuously be managed
through Ericsson's Responsible
Sourcing Program, the identified salient
risks will be addressed through more
focused, proactive and collaborative
engagements. Some of the identified
salient issues have direct bearing
on the human rights risks identified
through this 5G assessment process,
including occupational health and
safety (relating to rollout of physical
network infrastructure), right to an
adequate standard of living (relating
to workers potentially losing their jobs
due to robotization accelerated by 5G)
and conflict-related impacts (relating
to potentially increased demand for
conflict minerals).

Ericsson is currently in the process of
developing more detailed action plans
to respond to the identified risks. Risks
to human rights and the vulnerability of
workers in supply chains have become
more apparent during the current
COVID-19 crisis, which has hit the most
vulnerable people in the most severe
ways. Ericsson applied the explicit lens of
vulnerability, not just in the identification
of salient issues, but also in the rollout of
further actions as part of the Responsible
Sourcing Program.

[13] Find out more about supply chain human rights

Remedy and grievance mechanisms

According to the UN Guiding Principles, when Ericsson has caused or contributed to a human rights impact it has a responsibility to take action to provide or enable remedy. Where Ericsson is linked to an impact, it should apply leverage to move business partners in the value chain to take appropriate action, including to provide remedy.

Ericsson has acknowledged this responsibility in its steering documents, such as the Code of Business Ethics and the Business and Human Rights Statement. Developing grievance mechanisms and processes to implement this responsibility can also provide useful information to help track performance and identify and address impacts before they escalate into bigger issues for people and the company. As such, effective grievance mechanisms and a holistic approach to remedy is an integral part of human rights due diligence and implementing the UN Guiding Principles.

Ericsson has identified the need to further strengthen its approach to remedy and grievance mechanisms, to effectively address the full scope of human rights risks across its value chain.

One of the main challenges is to make sure that mechanisms are accessible to all stakeholder groups. As a network vendor, Ericsson does not have a relationship with individual end users that might be impacted. Its grievance mechanisms are therefore not well known or used.

The Ericsson Code of Business Ethics (CoBE) has been updated to better explain its responsibility to respect human rights and how complaints are addressed. Additionally, Ericsson is engaged in the B-Tech Project driven by the Office of the High Commissioner for Human Rights. A key component of the B-Tech Project is to identify how to establish effective grievance mechanisms in the ICT industry.

B-Tech Project
A key component is establishing effective grievance mechanisms in the ICT industry.

Monitoring, governance and stakeholder engagement

This section of the report covers how the identified impact areas will be addressed moving forward.

Many of the issues will need further analysis, sector-wide and multi-stakeholder collaboration, as well as re-evaluation as more is learned about 5G technology and potential human rights impacts.

Monitoring
For many of the impact areas, Ericsson already has internal processes and programs to monitor risk and actions taken; for example, the Sensitive Business framework, the Responsible Sourcing Program, the Ericsson SRM and environmental health and safety management systems. Through these established processes, Ericsson will continue to identify and address risks, as well as frequently evolve and strengthen its processes based on learnings.

In addition, based on the learnings from this assessment, Ericsson is in the process of establishing an updated human rights impact assessment methodology that will form the basis of future assessments. Such assessments can focus on country-level operations, new technologies or specific business engagements. The updated methodology will be piloted and refined through selected initial assessments.

Some of the impact areas, for example job transitions and digital inclusion, require actions and broader collaboration with external stakeholders, beyond Ericsson procedures. These impact areas will need further analysis in order to determine effective mitigation strategies.

As mentioned in the introduction to this report, this is an initial assessment based on what is currently known about human rights risks related to 5G technology. The listed actions respond to the identified impacts so far. By conducting this assessment, Ericsson has proactively engaged with relevant group functions and business areas to build awareness across Ericsson on human rights impacts connected to 5G. This engagement enables Ericsson to more effectively identify which functions within the company need to be engaged in addressing new and emerging risks within each impact area. It will periodically review actions taken and evaluate if additional actions are needed.

This will be done through engagement with appointed internal stakeholders for each impact area.

Governance
Many of the identified impact areas are already addressed through existing Ericsson programs, frameworks and processes, which are built on established governance structures with reporting lines and targets. As mentioned, some of the impact areas need further analysis to fully grasp how to develop effective strategies and governance structures to address these issues. Ericsson will continue to engage with internal and external stakeholders on these topics in order to develop a clear approach.

To ensure that the identified impact areas and suggested actions presented in this report are addressed, the cross-functional team of internal stakeholders that has contributed to this report will monitor progress within each impact area. Periodic updates will also be shared with external stakeholders to continue developing action plans for further mitigation.

While all of the existing Ericsson processes that manage identified risks will continue to feed into a periodical review of the findings of this assessment, in order to make sure emerging impact areas are identified early on, the cross-functional team will ensure that Ericsson has a centralized approach to 5G and human rights.

Stakeholder engagement

Stakeholder engagement was a crucial part of this 5G assessment process. The dialogue with external stakeholders enabled Ericsson to correctly frame the impact areas, "translate" the findings for various stakeholder groups, identify improvement areas in its processes and establish the groundwork for further engagement.

An important next step in acting on the findings of this report is to include external stakeholders in further developing preventions and mitigations. Ericsson will use this report as a starting point to engage external stakeholders on the topic of 5G and human rights, with the aim of building joint leverage and a common understanding across the ICT industry.

One challenge, already identified in the initial stages of this report, is to engage potentially affected stakeholders (people and communities whose human rights might be adversely impacted through Ericsson's business operations, products or services), in addition to expert stakeholders and credible proxies (organizations that can provide insight into the perspectives of affected stakeholders), especially in high-risk contexts. Working with peers and customers might be an effective way of addressing this challenge

and jointly engaging with potentially affected stakeholders.

Additionally, an area for further improvement is how to ensure stakeholder perspectives are more effectively included in existing frameworks and internal due diligence procedures. Other companies and organizations have for example established external stakeholder advisory boards, which can provide input and guidance on a more systematic basis.

Another area of improvement, which also enables better stakeholder engagement, is more detailed reporting on human rights, including as it relates to 5G. The publication of this report is an attempt to, in a transparent way, identify impact areas that need further engagement. Ericsson will actively engage external stakeholders on these topics and welcomes a constructive dialogue on how to further develop and improve actions taken.

In case of actual impacts, Ericsson encourages affected stakeholders to reach out to it with concerns through the Ericsson Compliance Line, or other channels where appropriate. The Compliance Line is available for internal and external stakeholders and covers human rights impacts connected to its business. As previously mentioned, Ericsson has identified a need to strengthen its grievance mechanisms to

ensure human rights are more effectively addressed. However, raising concerns through the Compliance Line will receive the proper attention.

Ericsson has a clear commitment, articulated in its Business and Human Rights Statement, to assume accountability by providing access to remedy in cases when it has caused or contributed to adverse human rights impacts and use its leverage with business partners if directly linked to such impacts.

Receiving and evaluating grievance is a crucial step in effectively managing the known impact areas and identifying new ones. Ericsson therefore welcomes stakeholder engagement through raised concerns and will work with stakeholders to identify appropriate remedy, as well as ways to further improve its grievance mechanisms.

Improvement
Ensure stakeholders' views are included in existing frameworks.

Communication and reporting
This assessment process is a key factor in identifying prioritized actions and improvement areas related to human rights across Ericsson's operations and value chain. The findings of this report will form the basis for further reporting on progress within the area of human rights and responsible business. Ericsson will track the performance of identified actions through its annual reporting, as well as periodical updates on progress where needed.

When new issues and potential impact areas emerge through Ericsson's due diligence procedures or through communication from and engagement with stakeholders, these will be included in its external reporting. By addressing the identified impact areas in collaboration with stakeholders, Ericsson ensures that progress is shared through ongoing dialogue.

While conducting additional human rights impact assessments — whether country or technology specific — Ericsson will further engage and report on actions taken in relation to the more specific context of each assessment.

Conclusion

While individual corporate responsibility is vital, the human rights challenges surrounding ICT must be addressed through a multi-stakeholder approach.

While this assessment report provides an overview of the potential human rights impacts connected to 5G technology, mainly from a network vendor perspective, the identified risks are relevant for the ICT industry as a whole to address. A clear conclusion of this assessment is that the identified impact areas to a large extent are cross-cutting, from both an internal Ericsson perspective and looking at the ICT industry as a whole. While individual company responsibility is paramount, the human rights challenges surrounding ICT must also be addressed through a multi-stakeholder approach. A single actor in the ICT ecosystem will not be able to effectively mitigate the full range of risks associated with 5G technology on its own.

While technological developments such as 5G undoubtedly bring substantial societal benefits, it is equally important to acknowledge the potential misuse and unintended consequences of such advances. Certainly, the relationship between human rights, ICT, law enforcement and national security is complex. At one end of the spectrum, technology delivers connectivity and empowerment and contributes to more transparent, safer societies. At the other end, unmitigated, unintended use of ICT can result in persecution, repression and human rights violations. It is important to keep these two perspectives in mind when developing, providing and using ICT solutions.

As part of Ericsson's responsibility to respect human rights, it needs to proactively engage with issues that can lead to adverse human rights impacts as a result of its operations, products, services and business relationships. Ericsson does not claim to have all the answers, or provide an exhaustive list of risks. But it believes that this assessment can form a strong foundation and starting point for the ICT industry to jointly establish a comprehensive approach to addressing human rights risks and inspire others to conduct similar assessments based on their operations and experiences. Only through shared learning, collective actions and transparent actions will some of the more complex challenges in the industry be effectively addressed.

Clearly defining respective roles and responsibilities is critical for developing a successful ICT ecosystem-wide approach in respect of human rights. By engaging with the entire industry, as well as focusing on Ericsson's own power to influence and shape the debate, it can better identify concrete steps that each actor in the chain can take to avoid or mitigate human rights risks.

Moving forward, Ericsson's focus will be broad dissemination of the report itself and targeted engagements with peers, customers, governments and civil society organizations to establish collaborations aimed at incorporating a comprehensive human rights approach in the rollout of 5G, as well as future management of the networks. By effectively mitigating and addressing human rights risks, Ericsson can truly leverage the positive impacts the ICT industry brings to the communities in which it operates and society in general.

Appendix

External stakeholders interviewed for this study

Access Now is a global civil society organization focused on digital rights. The engagement with Access Now centered on a broad range of emerging potential risks connected to 5G technology and a more connected society, as well as the role companies can play in mitigating risks at early stages of development of their products and solutions.

Vodafone Group is one of the world's largest telecommunications companies and provides a range of services including voice, messaging, data and fixed communications. The discussion with Vodafone mainly touched on the relationship between network vendors and mobile operators, identifying common risks but also distinct responsibilities.

The Global Network Initiative (GNI) is a multi-stakeholder initiative focusing on protecting and advancing freedom of expression and privacy rights in the ICT industry, by setting a global standard for responsible company decision making and serving. Ericsson is a member of the GNI and discussed with the organization the application of the GNI Principles in the context of this assessment process, as well as issues that have previously been raised through GNI learning calls, briefs and public engagements on the topic of 5G and human rights.

Telia Company is a mobile operator headquartered in Sweden, with operations across the Nordic and Baltic countries. The engagement with Telia Company focused on priorities from a mobile operator perspective and the impact areas that are well suited for collaboration, as well as the cases in which collaboration might be challenging.

Center for Democracy and Technology (CDT) is a civil society organization working to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. The organization has offices in the US and Belgium.

Meg Roggensack is an adjunct professor at Georgetown Law and expert on business and human rights. The engagement focused on risks related to digital inclusion, both from the perspective of coverage and connectivity and in relation to how technology could exacerbate human rights impacts due to existing factors such as structural inequalities and biases.

Jessica Fjeld is Assistant Director of the Cyberlaw Clinic at the Berkman Klein Center for Internet and Society at Harvard University. Some of the main topics raised as part of the engagement were the specific impacts on women of the identified risks, as well as potential ways to effectively regulate some of the impact areas.

Digital Rights Foundation is a research-based civil society organization working to strengthen protections for human rights defenders, with a focus on women's rights, in digital spaces. The organization is based in Pakistan and works throughout the region. The engagement focused on risks women face in connection to ICT, especially in Pakistan and neighboring countries.

Paradigm Initiative is a social enterprise that builds an ICT-enabled support system and advocates digital rights in order to improve livelihoods for under-served youth. The organization has offices in Nigeria, Cameroon, Kenya, Ghana, Zambia and Zimbabwe and works across the African continent. The engagement focused on perspectives and risks from the region, as well as examples of how companies and civil society can collaborate to promote digital rights.

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com