international journal of critical infrastructure protection 42 (2023) 100617

Contents lists available at ScienceDirect

International Journal of Critical Infrastructure Protection

journal homepage: www.elsevier.com/locate/ijcip

Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems

Paola Vargas *, Iris Tien

School of Civil and Environmental Engineering, Georgia Institute of Technology, North Ave NW, Atlanta, GA 30332, United States

ARTICLE INFO

Keywords:
5G
Critical infrastructure
Risk
Resilience
Cybersecurity

ABSTRACT

5 G technology promises a wide range of benefits for critical infrastructure (CI), including improved reliability, increased efficiency, cost savings, and increased worker safety. However, it also brings many new risks that CI owners and operators must be prepared for to facilitate effective risk mitigation and response. These risks, however, have not been systematically assessed for CI systems. This paper investigates how the cyber-physical risk landscape will be impacted by 5 G for four major CI sectors in detail: smart transportation, smart water, smart power, and smart oil and gas networks. Compared to prior work only examining a single CI network, the authors present a comprehensive assessment of the types of threats that these sectors can expect based on past incidents, the new vulnerabilities introduced by 5 G and existing vulnerabilities exacerbated by the introduction of more connected devices, along with mitigation recommendations for each risk. Risks associated with the rollout of and transition to 5 G, risks from 5 G network disruptions, cyberattack risks, and privacy risks are included. While each of the sectors has a unique risk profile, general themes also emerged across multiple CI networks. Notably, there will be an increased number of threat vectors from smart devices reliant on the telecommunications network to provide monitoring and control of infrastructure services. Because many of these devices are accessible by the public, the risk of social engineering attacks and vulnerability to physical hacking are exacerbated. Successful risk mitigation requires collaboration among CI's many stakeholders to implement security measures at the interfaces between connected devices to limit the access to assets in case one security measure is successfully bypassed. Due to the increased interdependencies between CI networks, operators must create backup plans to keep the most essential services running on a smaller bandwidth in case of a 5 G outage or similar failure. As 5 G capabilities continue to develop and the risk landscape evolves, ongoing research is needed and CI owners and operators should be prepared to update security measures to remain ahead of identified risks and threats.

1. Introduction

The fifth generation of wireless technology is upon us along with promises of ultra-high data transfer speeds and decreased latency to supply the increasing demand for high-quantity content to be delivered instantaneously. The transition from current 4 G LTE to 5 G is proposed to support a substantive shift in how information is transferred across the critical infrastructure (CI) landscape. It is anticipated to take us into a world where artificial intelligence and smart city applications are commonplace, with continuous monitoring of systems, communication of information with infrastructure owners and individual users, and automated control of these systems to achieve efficiency, safety, and sustainability objectives. However, before 5 G can deliver on its promises, a large-scale telecommunications infrastructure rollout and operational overhaul must take place to achieve a successful transition and provide the anticipated capabilities of 5 G. This growth and transition for 5 G is being done in a complex and risk-filled environment where the telecommunications network is subject to increasing threats while becoming increasingly integral in the operations of other CI. With increasing interconnectivity and interdependencies between CI systems, it is essential to consider the new risks that 5G-enabled features introduce for infrastructure network operations and recovery.

Technology is already being developed for the integration of 5 G into transportation, water, gas, oil, and other sectors which, if affected, can have devastating impacts on human health and safety. Because of the nature of the services provided by CI, it is essential to anticipate the

* Corresponding author.
E-mail address: pvargasvargas3@gatech.edu (P. Vargas).

https://doi.org/10.1016/j.ijcip.2023.100617
Received 5 January 2023; Received in revised form 3 April 2023; Accepted 20 June 2023
Available online 25 June 2023

types of risks that 5 G will bring in order to make plans to mitigate them. In this paper, the authors describe the challenges for various major smart CI networks in the transition to 5 G, as well as types of risks that can be anticipated from the increased interdependence with 5 G for these CI networks. Most previous work on infrastructure risk assessment focuses on physical risks, such as asset damages or physical deterioration. This paper additionally focuses on cyber risks, which are growing in importance in the analysis of CI risk and resilience [1,2]. While there has been work on cyber risks for a single system such as the smart grid, this work provides an assessment of risks across four major CI sectors to be able to assess commonalities and differences among systems. Included are smart transportation, smart water, smart power, and smart gas and oil infrastructure systems, which present a range of risk types for CI networks. These systems are selected as ones where 5 G is anticipated to significantly advance current operations and are of critical importance to the health, safety, and security of society. Analyzing four sectors allows the authors to find common themes across different sectors, while still allowing for an in-depth assessment of risk landscapes for the individual networks.

Throughout these technological advances, it is essential to maintain the confidentiality, integrity, and availability (commonly known as the CIA triad in information security) of the assets in critical infrastructure networks. In addition to investigating threats to data privacy (confidentiality) and threats aiming to tamper with assets (integrity) while keeping critical services up and running with appropriate parties in control of these networks (availability), this study includes an assessment of challenges specific to the transition period to 5 G, as 5 G infrastructure is built out and automated features gradually become available. For each of the four CI sectors studied, this paper goes into detail for the risks associated with the transition to 5 G, cyberattack risks, and privacy risks, all risk types that are becoming increasingly prevalent with expanding system connectivity and operations at the edge. While many prior works have investigated the cyber-physical risk landscape of a 5 G telecommunications system, this study seeks to understand the cascading risks that 5 G brings to CI networks that will use it. Compared to purely qualitative studies, this study includes quantitative measures of the sizes of infrastructure systems, uses of 5 G, and descriptions of prior historical events where possible to provide a sense of the scale of potential risk impacts. From the identified risks, this paper also describes the authors' recommendations for mitigating these risks, building on existing works describing the applications of 5 G in CI networks and some of the security concerns associated with these applications. This paper provides for the first time a comprehensive overview of the risks associated with the transition to 5 G for four CI systems, as well as an assessment of particular elements of the risk landscape after the transition. This new landscape will include not only 5G-specific risks, but also existing risks that may be exacerbated by the increase in connected devices that comes with the implementation of more smart features. This paper provides a foundation, given the information currently available in the early stages of 5 G implementation, for stakeholders to consider their systems' cyber-physical vulnerabilities, and the types of risks that each network may face. It provides a basis for designing 5G-enabled features with these risks and vulnerabilities in mind to minimize these risks even before the features become functional.

The rest of the paper is organized as follows. The next section describes the connections between the telecommunications system and other CI networks, highlighting the criticality of investigating the intersection and interdependencies between these systems. Previous work in this area is then described, where a gap is identified in assessing the impacts of emerging 5 G technologies on CI risk assessment. Next, the authors summarize the functionality and capability advances of 5 G, including the anticipated benefits of the 5 G network as it relates to enabling functionality in other CI sectors, and risks specifically arising from the transition from 4 G to 5 G. The following sections then describe the risks associated with specific major smart CI systems analyzed, including smart transportation, water, power, and gas and oil networks. For each of these systems, risks during the rollout of 5 G, risks in the case of a 5 G network disruption, cyberattack risks, and privacy risks are examined. The authors discuss each CI system individually along with corresponding mitigation recommendations and common themes across sectors.

2. Telecommunications and critical infrastructure

Infrastructure systems provide varying services that are critical to the safety, security, health, and efficiency of society. Among these functions, the communications sector provides access and connectivity capabilities, enabling the function of many other critical systems such as energy, water, transportation, and emergency services that depend on communications for operations and recovery. The dependence of CI sectors on network communications is continuing to grow as these systems become more connected and automated, and the number of applications and services for monitoring and control that require a network connection increase. These changes in how infrastructure systems operate, however, increase the criticality of telecommunications not only for the communications sector, but for its dependent CI sectors as well. One result is that a communications disruption could lead to disruptions of other critical sectors, resulting in potential cascading failures due to these dependencies [3,4] and compounding the infrastructure impacts while trying to recover the network after a disruption.

The implementation of 5 G for the telecommunications network is central to this increase in the reliance of other CI systems on network connectivity. For example, 5 G is enabling machine-to machine communication and increased smart infrastructure monitoring and control. Such capabilities depend on a reliable network connection to function properly and a resilient connection to continue to function through disruptions. The wide-ranging dependencies of CI systems on telecommunications infrastructure is shown in Fig. 1. Included are the varying sectors reliant on telecommunications, and the functions within each of those sectors that utilize telecommunications for operations. Disruptions to the telecommunications system could severely impact these critical sectors and functions as shown in Fig. 1, including operations in the energy, manufacturing, emergency services, finance, public health, water, and transportation systems. Of these, transportation, water, energy, and gas/oil systems are the focus of this study as critical systems to support society.

With these connections, vulnerabilities in the telecommunications system translate into increased risk to CI systems. The use of telecommunications infrastructure to identify and communicate anomalies and disruptions to a system makes telecommunications infrastructure vital in ensuring not only infrastructure reliability but also CI resilience. With a broadly accepted definition of resilience as the ability to "prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [5], telecommunications infrastructure is critical to infrastructure resilience across sectors and aspects of resilience. Increased remote monitoring and control of infrastructure assets makes communications essential to first quickly identify system faults or failures - addressing the ability to absorb the effects of an adverse event - and then to deliver patches or deploy fixes to bring the system back online - addressing the ability to recover from disruptions [6]. As infrastructure owners, national agencies, and academic researchers seek to increase infrastructure resilience, it is critical for these stakeholders to understand the risks associated with the various components of the telecommunications network, including throughout the transition from 4 G to 5 G, to be able to mitigate and protect against those risks.

3. Background and related work

Extensive work has been conducted in the field of risk analysis of interdependent infrastructure systems. Applegate and Tien [7] propose a Bayesian network-based approach to probabilistically assess

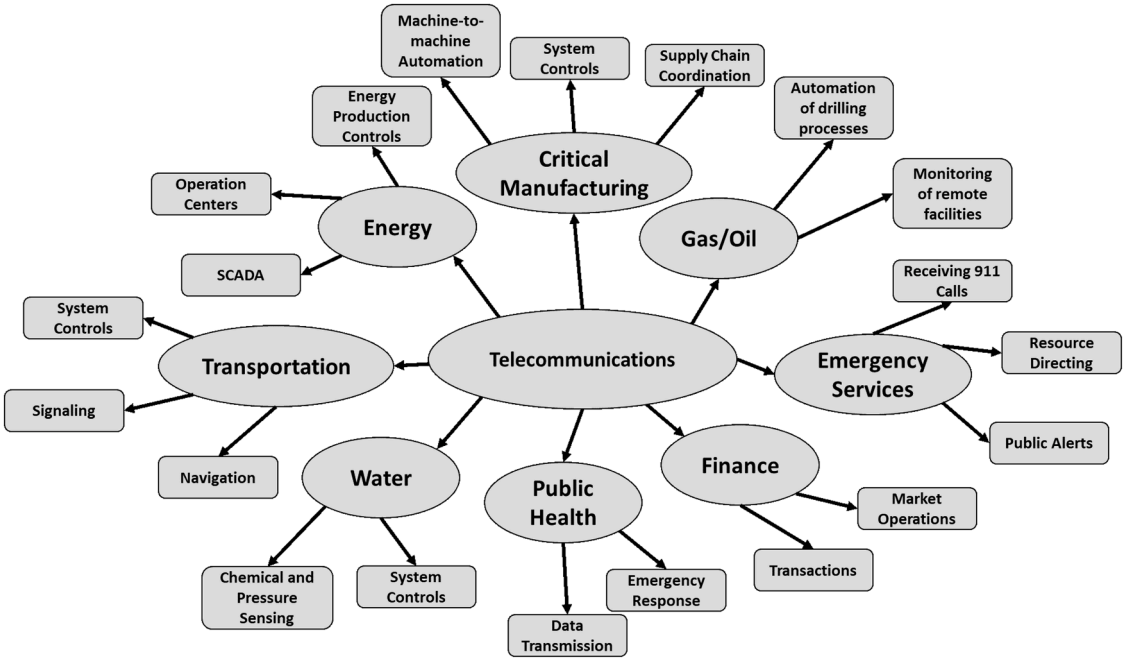

Fig. 1. Overview of CI sectors and functions dependent on the telecommunications system for operations and recovery.

infrastructure interdependencies. Suo et al. [8] present a method to probabilistically quantify CI risk, which uses expert opinion to take into account interdependencies between CI networks. Kim et al. [9] assess the risk to the industrial control systems used in many CI applications, highlighting the cascading impacts on dependent networks. While these approaches can be applied to the risk assessment of CI systems dependent on telecommunications networks, most of these are generalized approaches that may not account for the specifics of telecommunications systems. In addition, the methodologies often require large amounts of detailed data about components that is not available for 5 G network applications in CI that have not been constructed or in some cases designed yet.

Johansen and Tien [4] introduce the idea of access for repair infrastructure interdependencies, which characterize infrastructure components that must be functioning to provide access to repair failed components in other infrastructure systems. Included is the idea of cyber access provided by telecommunications infrastructure to be able to connect and communicate with CI components. However, a generalized modeling framework to capture these access for repair interdependencies is described, rather than detailing the specific risks arising from increased cyber and communications connections.

In the area of cybersecurity research, there have been limited studies on the connections between cyberattacks and other CI sectors. Hassanzadeh et al. [10] and Huq et al. [11] summarize cybersecurity incidents in specific sectors (smart water and smart transportation networks, respectively), which help to identify trends across the types of attacks that have occurred in the past and the trends in objectives of attackers targeting each CI sector. Kimani et al. [12] present a series of cybersecurity risks that smart grids face as the energy sector becomes more integrated with the internet of things. However, these do not give information about how 5 G technology specifically will change the risk landscape. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) [13] has summarized potential threats to the telecommunications network. However, this assessment does not include risks to CI networks that depend on 5 G to function.

Various studies investigate the privacy and cybersecurity risks that 5 G networks will face along with recommendations for how to mitigate them [14,15] but do not extend the risk assessment to the other critical networks that will be interconnected with the telecommunications network. Borgaonkar et al. [16] evaluates cybersecurity for the 5G-enabled smart grid. However, only the grid network is analyzed, without consideration of other CI. Lai et al. [17] investigate the privacy and security risks that 5 G brings to a smart traffic network through analysis of a case study as well as a qualitative summary of current challenges in 5G-enabled smart transportation networks. Compared to these prior works, this paper presents the first study of its kind to comprehensively assess the risks of 5 G to several connected smart CI with quantitative estimates of the impacts based on relevant past incidents, and special consideration for the transition period during which 5 G infrastructure is being developed and deployed. It details the role that 5 G will play in smart CI for four major sectors (transportation, water, power, and oil and gas), describes properties relevant to its applications in CI systems, outlines the risk landscape for 5G-enabled smart CI, and presents mitigation recommendations to address these risks.

3.1. Advances of 5 G and its uses in critical infrastructure systems operations and recovery

This section describes the functionality and capabilities of 5 G, including the anticipated benefits of the 5 G network, particularly as they relate to enabling functionality in other CI sectors. One of the key advances in 5 G is its support of increasing data volumes and speed. 5 G will significantly increase the estimated maximum amount of data throughput available from the current 100 Megabytes per second (Mbps) of 4 G LTE to 20GBs per second (Gbps) [18]. A faster throughput will enable increased data speed and capacity with anticipated benefits to CI, such as near real-time monitoring of assets such as pump conditions for a water distribution network or traffic conditions for transportation systems.

To meet the demand for increased capacity and throughput, an expanded spectrum of radio frequencies will be implemented with 5 G to reduce data congestion. This increased frequency range, or bandwidth, is vital to support the growing Internet of Things (IoT), with devices that are connected and communicating with each other to perform certain tasks, without necessarily requiring human-to-human or human-to-computer interaction [19]. 4 G LTE uses a relatively small frequency range typically around 2 to 6 GHz. If a large number of connected devices attempt simultaneous access to the same limited spectrum space,

then queueing issues and capacity limits will decrease the quality of service provided. Data congestion results, exceeding the capacity of the system and preventing data requests from going through. This is particularly problematic when many devices are in close proximity attempting access to the same bandwidth or same node into the network at once, as is proposed for many smart city applications with distributed sensing, data processing, and communication. 5 G addresses this issue by expanding the amount of spectrum available for telecommunications providers to lease for connected devices. This will be valuable in applications such as smart water networks and smart energy, where large amounts of smart sensors and meters will be transmitting data continuously and simultaneously.

In addition to faster and higher capacity throughput, a decrease in latency is another key feature of 5 G that is of relevance for CI sectors. Current 4 G latency is about 15 microseconds (μs), while 5 G seeks to decrease latency to under 1 μs [20]. Ultra-low latency is crucial to services that 5 G looks to provide. For instance, autonomous vehicles do not require high throughput speeds; however, low latency is essential to their successful operation. Self-driving cars do not demand high amounts of data to function but must have instantaneous access to communicate with other vehicles to ensure safety and functionality. Expanding the spectrum for 5 G will support both the high throughput and low latency advancements of 5 G. This will be accomplished by using higher band frequencies above 24 GHz in addition to enhancing current 4 G frequencies.

The different radio bands can be broadly divided into three categories: low-, mid-, and high-band radio frequencies. Each band frequency range is tasked with meeting different 5 G needs. Low-band frequencies will be used to enhance existing 4 G LTE spectrum applications and the current mobile broadband environment. This will allow faster data throughput to mobile devices and greatly increase the capacity of high data-consuming activities. Mid-band spectrum will be tasked with supporting Ultra-Reliable Low-Latency Communications (URLLC). This is intended to enable specific applications such as autonomous vehicle transport and monitoring the condition of water distribution pipes. Finally, the high-band spectrum range will support massive Machine Type Communication (mMTC) to ensure many IoT devices will have a reliable connection. Millimeter-wave (mmWave), a subset of the high-band spectrum range, provides the fastest data transfer rates.

The multiple bands for 5 G will be integral in supporting CI systems for monitoring in smart infrastructure and smart city applications, as well as for enhancing quality of service in densely populated areas [21]. There are, however, challenges and limitations to expanding the radio frequency spectrum, including in the CI applications that will utilize the expanded bands. In the lower band frequency spectrum on which 4 G LTE operates, waves can propagate over long distances and penetrate through buildings and other obstructions. C-band is a frequency band (3.4 - 4.2 GHz) within the mid-band spectrum that is considered especially valuable because it provides a favorable combination of the speed of higher frequency signal and the range of lower frequency signal [22]. The higher frequency spectrum increases performance with higher throughput capacity and lower latency characteristics; however, waves in these frequencies travel shorter distances and can be blocked by obstructions and even be affected by inclement weather conditions [23]. Waves in the high-frequency band are easily blocked by surrounding buildings, and therefore require more densely placed infrastructure to achieve consistent coverage [24]. Because this is not feasible over large areas, high-band service is expected to be limited to small, densely populated urban areas, while rural areas will likely be limited to the

Table 1
5 G bands: advantages, disadvantages, and uses for critical infrastructure systems.

Band name	Low-band	Mid-band		High-band
Frequency Range	< 1GHz	1 - 2.5 GHz	3.4 - 6 GHz	24 - 86 GHz [28]
Mobile network technology standard that uses band	2 G, 3 G, 4 G, **5G**	2 G, 3 G,4 G, **5G**	4 G, **5G**	**5G**
Advantages	Travels further: Each antenna has wider coverage Can provide nationwide coverage [25] Can travel through physical obstacles [25] Can use much of existing 4 G infrastructure for 5 G deployment	Wider usable spectrum: capacity for more devices than other bands [24] Can travel through walls [24] Optimal balance of wider coverage per antenna and higher speeds [24]	Contains C-band spectrum (3.4 - 4.2 GHz) [26]	Contains mm-Wave frequencies used by telecommunications companies (28 GHz and 39 GHz) [29] Ultra-low latency / high speeds Suitable for many valuable applications such as vehicle automation due to high speeds
Disadvantages	Lower speeds than mid- and high-band	Because of the popularity of this frequency band for uses other than 5 G, securing sections of the spectrum at auctions is difficult and expensive for service providers [24] Must ensure that 5 G in this band does not interfere with other users (e.g. Federal Aviation Agency concerns about interference with airplane safety equipment) Lower speed than mm-wave: not optimal for many applications that require near real-time connectivity [27]		Cannot travel through walls [24] Other physical obstacles (e.g. glass, vegetation) can interfere with signal Travels shorter distances: more infrastructure required Coverage will be limited to small, densely populated areas [24]
Uses for critical infrastructure systems	Monitoring of resource consumption (electricity, water) using smart meters Monitoring of system components to determine when/where maintenance is required Accommodating the large number of smart devices connected to smart power grid			Near-real time transmission of sensor information from vehicles over a short distance (automobiles, ships, etc.) [30] Real-time communication with field workers during specialized repairs

mid- and low-band spectrum. This will have implications for the CI services enhanced by 5 G as well. The properties of the varying bands including their uses for CI systems are summarized in Table 1.

Finally, to achieve the proposed advancements of 5 G will require a robust set of hardware and software components to be rolled out and operationalized to ensure that quality of service and connectivity requirements are met. To achieve usable high frequency data transmissions, 5 G will implement small cell devices that act as miniature base stations to provide short distance coverage. The range of small cells will be between 10 m and a few hundred meters depending on use and obstructions in the line of sight between the node and the device. Small cells will need to be placed every 250 m on average in urban areas to achieve the quality of connection desired [31,32]. The small cells will increase the number of connected devices that are able to connect to a given tower, and greatly increase data throughput capabilities.

While each of these components enhances 5 G capabilities, each also introduces new risks to the telecommunications system. One of the purposes of this paper is to highlight the emerging risks associated with the increasing use of 5 G for CI so that research can be conducted, and mitigation measures put into place before the full deployment and operations of these systems. There is, however, a transition period for this to happen, which itself is subject to certain risks. These are described in the following section, which discusses the current rollout progress and risks specific to this transition period.

3.2. Transition from 4 G to 5 G and associated risks

Because of the large amount of infrastructure needed for the full implementation of 5 G technologies, the rollout of 5 G is planned to take place in phases. Initial 5 G rollouts will rely heavily on the existing 4 G network, referred to as a non-standalone (NSA) 5 G network. Over time, rollouts will build towards a standalone (SA) 5 G network, which has its own core network independent of 4 G [33]. While beginning with a NSA network allows providers to begin to provide enhanced service to customers before the full 5 G network is built out, it also means that the NSA network will inherit much of the risk landscape of the previous 4 G network. These risks include vulnerability to viruses that can cause reduced signal speeds or leaks of personal information [34], and greater susceptibility to denial-of-service attacks [35]. Considering the multiple bands of 5 G as described in Table 1, Fig. 2 describes the general rollout strategy for 5 G and current progress as of this writing.

Large companies such as AT&T have prioritized making high-band signal available in venues (e.g., stadiums, airports) in major cities before expanding to larger areas [36]. Though all three bands identified in Fig. 2 are already being rolled out to some degree, the general strategy of providers is to start with expanding the bandwidth of low-band signal by building on existing 4 G LTE infrastructure, and then building out mid- and high-band infrastructure [33]. AT&T offers low-band signal in many cities, is working on mid-band (C-band) and is slowly building out high-band in densely populated areas.

Because more high-band infrastructure is required than for mid- or low-band, coverage expands most slowly for high-band service. Additionally, with the high initial cost of installing the antennas required for 5 G signal [34], and as telecommunications companies cannot expect a very high number of 5 G subscribers from the beginning, the amount of money that providers can put into expanding their infrastructure is limited. This not only constrains the quality of service that companies can provide to 5 G customers initially, but it also limits its applications for CI systems if the necessary speeds are not available consistently. For example, in the early stages of rollout when high-band signal is only available in a few public venues nationwide, a connected vehicle as part of a smart transportation network cannot rely on 5G-enabled automated features to communicate information with nearby roadside units throughout its entire trip. Even in later stages, when high-band signal is available throughout cities, coverage cannot be guaranteed along all roads and highways in the country. This means that 5G-enabled automated driving features will only be able to be implemented once there is high-speed coverage over a large area, and there must be backup processes in place for use where 5 G is not yet built out or when 5 G signal is disrupted.

With the amount of infrastructure needing to become operational for a full 5 G rollout, there will be differentials between locations of implementation. In addition to varying implementation of bands of signal across providers, there is the potential of increasing the “digital divide” and inequality in the access to technology among a population [35]. Because it is least cost-effective for companies to provide mid- and high-band signal in rural areas, people in urban areas will have better access to higher speed signals than those in rural areas. Critical

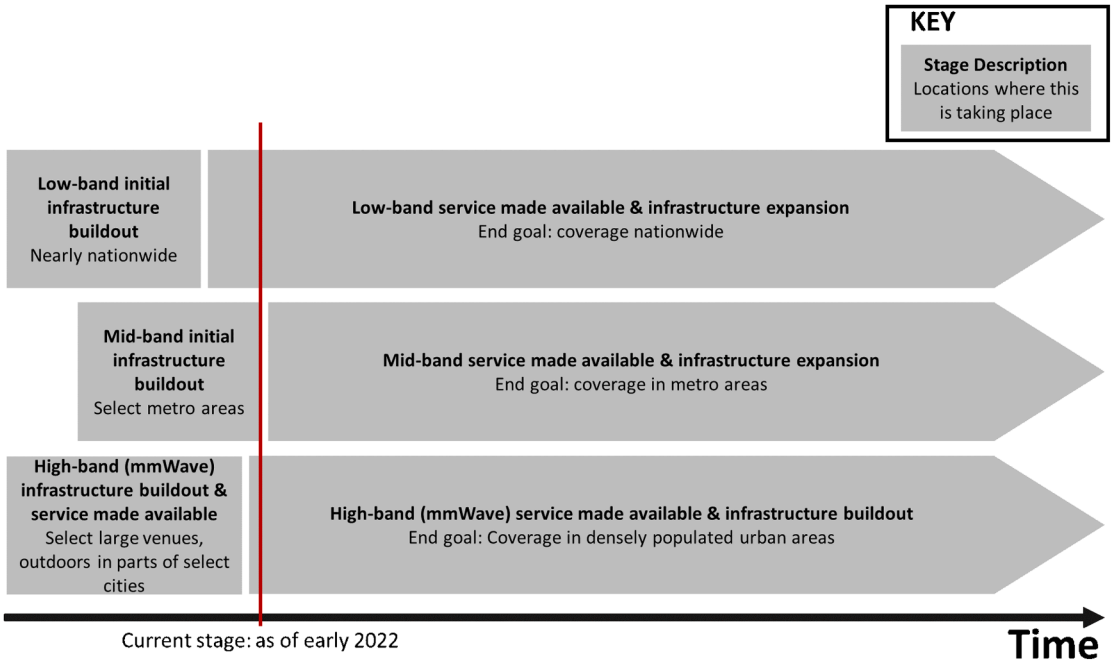

Fig. 2. 5 G rollout process and current progress.

infrastructure utilities in densely populated cities will have earlier and better access to 5G-enabled features, while utilities serving smaller, rural populations will not have access to the same benefits. This widens the digital divide because the benefits enabled by 5 G for CI will be limited to certain populations.

Finally, there have already been operational risks identified and encountered in this early phase of 5 G implementation and with current rollout progress. In early 2022, the aviation industry voiced concerns that 5 G C-band signal could interfere with safety equipment used by airplanes [36]. Providers AT&T and Verizon had planned to begin rolling out C-band service on January 4, 2022. Once the security concern was voiced, however, at the request of the U.S Secretary of Transportation, AT&T and Verizon agreed to push back rollout two weeks to allow time to assess the risks that 5 G poses to aviation. As the rollout of 5 G continues to take place, it is likely that further security concerns will emerge that highlight risks between the telecommunications and other sectors and can cause costly delays for telecommunications providers. This incident highlights the importance of anticipating risks as well as collaborating with other industries to avoid such last-minute setbacks and ad-hoc risk mitigation measures. The next section details the specific risks posed by 5 G in the operations and recovery of smart CI systems, specifically for the four major sectors of smart transportation, smart water, smart power, and smart gas and oil infrastructure.

3.3. Risks of 5 G for smart critical infrastructure systems

For each of the four systems examined (smart transportation, water, power, and gas and oil networks), risks from 5 G in each of the following three categories are examined: 1) Risks during the rollout of and transition to 5 G and risks in the case of a 5 G network disruption; 2) Cyberattack risks; and 3) Privacy risks. These networks present a range of risk types and historical risk scenarios. The authors first discuss each CI network individually along with corresponding mitigation recommendations and then present common themes across sectors.

3.3.1. Smart transportation

Current advances in the transportation system are based on the ability of 5 G to provide near real-time communications with low latency. The transportation sector will make use of 5 G to allow vehicles to gather information about their surroundings as well as enable communication between a vehicle and surrounding vehicles, infrastructure, and pedestrians [37]. This technology, i.e., cellular vehicle-to-everything (C-V2X) communications, promises many benefits in terms of traffic security and efficiency by allowing for various levels of vehicle automation [38]. However, transmitting sensitive vehicle information and eventually using 5 G to control the movement of vehicles means that there are severe privacy and safety concerns in the event of a failure, malfunction, or cyberattack on the 5 G network. Additionally, vehicle communication and automation require near real-time signal speeds so that vehicles can react quickly to their changing environments, which requires high-band (mmWave) signal.

3.3.1.1. Risks during transition to 5 G and risks in the case of a 5 G network disruption. Even as high-band 5 G infrastructure is rolled out in more parts of major cities in the near future, coverage will be limited and inconsistent due to the short range of high-band antennas. This means that the areas in which vehicles can send and receive messages with low latency will be spotty, which can be dangerous if a driver is reliant on the vehicle's automated features. With the focus of high-band rollout in urban areas, vehicles may not have high-band enabled automated features throughout their entire trip, especially in rural areas, in suburban areas, or along highways. Drivers in vehicles with automated features have been found to have reduced situational awareness due to increased reliance on the automated driving assistance features [38]. Inconsistent signal can cause safety concerns if the driver is counting on the vehicle's assistance with lane changes, emergency braking, or other critical functions. In the case of a 5 G network outage, the concerns would be similar to those just described.

During the 5 G rollout process, vehicles on the road can be expected to mostly have lower levels of automation, meaning that vehicles have automated features that help drivers with certain tasks such as lane changes or parallel parking, but the driver is still fully responsible for the operation of the vehicle. Since the driver is still mainly in control of the vehicle, the consequences of a lack of 5 G coverage, inconsistent coverage, or a 5 G network outage are likely not as severe as with higher levels of automation, where the vehicle is directed and controlled automatically. As 5 G network coverage increases and automated vehicle features and capabilities increase, however, the implications of increasing dependence of vehicles on 5 G must be taken into account. For example, during this transitional period, to avoid safety hazards, it is essential to keep the driver alert and in control of the vehicle. This can be done by sending clear alerts to the driver when mmWave signal is interrupted and automated features are no longer reliable, so that the driver can react accordingly.

3.3.1.2. Cyberattack risks. The human safety element of smart transportation systems makes the potential impacts of a 5 G network cyberattack particularly significant. There are cases in which attackers can alter any of a range of C-V2X messages, including between vehicles, and between vehicles and infrastructure, causing unpredictable behavior in vehicles. The two most common types of messages sent using C-V2X technology are Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM). These types of messages are intended to communicate information about a vehicle's position coordinates, direction of movement, information from the vehicle's environmental sensors, identification as a public vehicle (school bus, etc.), among other detailed information [39]. This can be useful to help other vehicles identify and avoid hazardous conditions or simply avoid areas with heavy traffic. If any of these messages are altered, however, the automated features of a vehicle can be based on incorrect situational information. For example, if a CAM communicating the distance between vehicles is altered, this incorrect information will impact the outputs of automated vehicle-following algorithms, leading to potential crashes and significant life safety impacts.

Roadside units (RSUs) receive CAM and DENM from vehicles and distribute alerts about obstacles on the road, traffic congestion, etc., to the relevant vehicles. A cyberattack targeting a RSU can cause widespread changes in the behavior of many vehicles at once. Thus, it becomes even more critical to assess the risks associated with these infrastructure assets. Consistent monitoring of RSUs for suspicious activity is essential to quickly identify and fix any malicious code or communications that may impact a large number of vehicles. Because the behavior of one vehicle affects that of nearby vehicles and can easily cascade to network-level impacts, it is difficult to predict the extent of the consequences of such an attack. Efforts have been made to use RSUs to monitor vehicles within their range and detect suspicious behavior, for example through a challenge-response authentication that can detect malware in a vehicle without transmitting additional private information between the vehicle and RSU [40]. A similar approach may be beneficial for monitoring RSUs, either periodically by vehicles or by other RSUs if their signal ranges overlap. Detailed analyses of risk scenarios are useful for understanding the effects of attacks on both network efficiency and passenger safety. Such analyses, including micro-level simulations, can be tailored to a specific location of interest and the automated features available, enabling specific quantitative assessments of potential risk impacts to the network [41]. Simulations like these may also be used to test various mitigation efforts in a cost-effective way to determine which to implement.

In addition to vehicles and RSUs, other infrastructure connected with smart transportation networks, such as digital signs, are targets of

hacking. Previous instances of these attacks include the removal of a construction site warning message on a digital highway sign by a person who guessed the login information to the controls of a digital sign. Although this was intended as a prank, the safety of construction workers was put at risk [11]. In another similar incident, an attacker gained access to digital road signs owned by a private contractor and changed the message displayed [11]. While these were not 5G-enabled, the automation of more infrastructure located in areas easily accessible by the public makes it more difficult to provide enough physical security to all distributed infrastructure assets supporting a smart transportation system to prevent such attacks.

3.3.1.3. Privacy risks. Transmitting the detailed information contained in CAM and DENM across the assets in a smart transportation system introduces privacy risks to network users. Accessing information about a vehicle's location or destination would allow a malicious actor to track a vehicle's movement along roads. This could lead to safety and privacy concerns for the vehicle passengers, who are unaware that they are being tracked. Other possible attacks include side-channel attacks or passive man-in-the-middle (MITM) attacks in which an attacker can access messages sent by vehicles and access private information. Such risks comprising private information in a 5G-enabled system exist across the CI sectors examined, as discussed in the sections following. What distinguishes the privacy risks for the smart transportation system is the dynamic nature of the information being shared, with mobile assets, i.e., vehicles moving throughout the system, and the number of interactions and communications among the components of the system.

3.3.2. Smart water

As the technologies for smart water systems advance, water distribution networks will use sensors to monitor the condition of infrastructure such as pipes to identify leaks or prioritize pipes for maintenance [42]. Other applications include detection of blockages in sewage systems, smart valves and pumps that adjust to changes in flow rate, and smart meters in streets and at homes [42]. Smart meters track water usage in near real-time and provide water treatment plants detailed information about demand throughout the day, making it easier to detect leaks, bill customers more accurately, and encourage customers to save water through consistent reports of their usage [43]. While some of these features are already being used, 5 G will allow more features to be functioning at once due to the larger bandwidth, more reliable communication between devices, increasing the effectiveness and number of simultaneous use of smart components [42]. Edge computing technology associated with 5 G will also allow more data processing to be done at edge devices such as water meters instead of transmitting all collected data to the server and sending processed results back to the device, further improving efficiency [44]. However, edge computing brings new security concerns. Importantly, user devices (e.g. smart meters at homes) increase the vulnerability of the smart water network to private information theft or hacking due to lack of physical security. In particular, previously centralized assets can be more consistently secured compared to the distributed assets of an edge computing network. Using this type of computing infrastructure securely requires securing of multiple edge servers, which can be more costly than concentrating security measures around one central server [45].

3.3.2.4. Risks during transition to 5 G and risks in the case of a 5 G network disruption. The main challenge during the transition to 5 G will be the limited availability of 5 G infrastructure. At first, 5G-enabled smart water features will be limited to select large cities and less accessible to small towns and rural areas. The initial cost of the sensors and smart meters may also inhibit smaller water treatment plants from implementing this technology. This keeps smaller, more rural communities from benefiting from the advantages that 5 G offers for utilities, increasing the digital divide between more affluent, urban communities and low-income and rural communities.

During a potential 5 G network disruption, smart water networks would have to rely on more manual monitoring methods or use 4 G as a backup. Using 4 G would mean that there would be no real-time sensor updates and that the overall bandwidth would be reduced. This would likely mean that not all smart devices could be kept online, even at lower speeds. As reliance on 5 G network capabilities increase, for a case like this, smart water utilities should have an emergency plan prioritizing which functions can or must continue running on the limited bandwidth and signal speed provided by 4 G, and which functions can be done manually until 5 G service is restored.

3.3.2.5. Cyberattack risks. Water systems have already been the target of cyberattacks. A water treatment center hack attempt in Florida in early 2021 targeted the chemical levels in drinking water. In this case, rapid detection allowed an employee to manually fix the issue before it affected the public. A Pennsylvania water plant saw similar attempts and stated that hacking attempts are becoming more frequent with the goal often being to damage components such as pumps or valves [46]. Such attacks put the populations served by these water treatment plants and distribution systems at risk. The Pennsylvania plant attack, for example, put the health of the occupants of the 2300 homes and businesses serviced by the plant at risk. Additionally, if successful, an attack could require the drainage of water reservoirs if the quality of the water is tampered with, causing significant economic and environmental consequences [46].

Other cyberattacks on water infrastructure include ransomware attacks. Several ransomware attacks have occurred on water plants throughout the U.S. over the last few years. An attack in Nevada in 2021 infected main monitoring and control systems as well as backup systems. Similar attacks occurred in Maine and California in 2021, as well as New Jersey and Kansas in 2020 and 2019 [47]. Ransomware attacks aim to benefit the attacker financially, causing potentially debilitating financial losses for utility companies. While the Public Utility Commission requires annual cybersecurity plans of large utilities, it does not require this of smaller ones [46]. New regulations aim to close this gap; however, implementation remains ongoing. There are presently over 148,000 drinking water systems in the United States, with only 9% of these servicing over 257 million people. The remaining 91% are much smaller, providing water to populations of under 10,000 each. Because America's Water Infrastructure Act of 2018 requires water networks providing water to at least 3300 people to have up-to-date risk assessments, smaller networks who do not have updated risk assessments are left especially vulnerable [48]. Increasing accountability for smaller utilities to consider their cybersecurity threats through policy or defined best practices will prepare them for the evolving risk landscape. At the same time, malfunctions of or targeted attacks on one of the largest 9% of plants can impact millions of people, making them prime targets for malicious actors seeking ransom money or to cause large-scale harm. As seen from prior events, early detection and employee intervention is instrumental in preventing severe consequences of potential cyberattacks. Increased investment in security measures to quickly detect unusual activity and alert on-duty employees is recommended to maintain control over the 5G-enabled automated features and reduce risks associated with increasing cyber connections.

3.3.2.6. Privacy risks. Installing smart meters means that detailed information about a household's water consumption is gathered. While this may not seem like especially private information, water consumptions of zero during the same time each day can indicate to a malicious actor residents' work or school schedules and no water consumption over a prolonged period of time may suggest that residents are on vacation or that the residence is vacant. This can be used to plan targeted break-ins. Although edge computing improves efficiency, it also results

in more consumer information being processed and aggregated close to the devices located in neighborhoods. This increases the consequences of physical attacks because it not only creates more access points for attackers but also increases the amount of personal information available at these devices [33,36]. In addition, providing these data to consumers through their accounts makes users more vulnerable to social engineering or phishing attacks, where attackers seek to obtain login or financial credentials. To prevent this, it is essential to treat any outside users as untrusted within the system and limit what is able to be accessed through individual accounts.

3.3.3. *Smart power grid*

The anticipated advances for smart power networks from the advent of 5 G is similar to those for smart water grids. Smart power grids are planned to benefit greatly from in-home smart metering devices that will track energy consumption throughout the day [49]. This increases the efficiency of the network by informing providers of energy demands, allowing them to optimize their energy purchases from producers as the electricity market price changes hourly. Additionally, providers can more easily manage power supplied from a larger number of smaller sources, making it easier for renewable energy producers to be integrated into the grid. Other smart applications in the power grid include automatically detecting and powering off idle base stations to save energy [50].

Currently, the average duration of blackouts in the U.S. is about 100 min, and an average of roughly 8000 people are affected per outage [51]. Smart power grids are expected to increase reliability (decreasing the average duration of power outages and the average number of customers affected) through features such as advanced metering, automatic fault location, isolation and service restoration, as well as automatic switching devices [51]. Though 5 G is anticipated to provide significant environmental and economic benefits to the power grid, it also introduces a variety of new risks for which infrastructure owners and operators must be prepared. Though only four cybersecurity incidents on the power grid have been reported, the frequency of these events is expected to increase in the future [52].

3.3.3.7. Risks during transition to 5 G and risks in the case of a 5 G network disruption. Ownership of the power grid is split among a variety of owners. While some parts are public utilities, others are owned by investors, independent power producers, or other government agencies [52]. Investor-owned utilities (which make up only 6% of the total) supply energy to 72% of U.S customers. This means that many stakeholders must be on board and willing to make the initial investments needed to implement 5G-enabled smart features. The result is that implementation of these features is likely to vary widely among different parts of the power grid, resulting in different vulnerabilities and security measures throughout. Interconnections between parts of the grid also need to be considered to ensure consistent functionality across local grids and that vulnerabilities do not propagate across portions of the grid. In addition, the large amount of IoT devices connected to the power grid at homes with a wide variety of security features, including some with no cybersecurity measures at all [53], results in vulnerabilities at the interfaces between different parts of the network that are difficult to predict. The multiple parties involved in grid operations and functionality highlight the need for collaboration among many to secure the grid. Standardized security features across providers and, as much as possible, for IoT devices is valuable in managing these vulnerabilities. Initiatives to standardize IoT security measures have helped close some of the security gaps between connected devices, but challenges remain relating to interoperability and security at the interfaces between devices [54]. Because of this unpredictability, devices connected to the smart grid must be treated as unreliable entry points. Alladi et al. present a list of smart device vulnerabilities, cyberattacks that can exploit these vulnerabilities, and corresponding countermeasures that can be employed to protect against such attacks [55]. The authors also highlight the need for consistent security patching as cyberattacks evolve [55].

While the 5 G network is non-standalone, it is less likely that 4 G will still be available to be used as a backup in the case of a 5 G network outage as this 5 G implementation is already heavily dependent on the existing 4 G network. If the 5 G network is compromised in this case, the 4 G network for which it is an extension cannot be relied on to be a backup. Once 5 G is a standalone network, it will operate independently of the 4 G network, making it unlikely that both will be compromised simultaneously. Smart power grids can then rely on the 4 G network as a backup in case of 5 G outage or denial-of-service (DoS) attack [16]. Existing smart power grid features (not using 5 G) are already effective in increasing reliability. Georgia Power reports that its smart power grid features have prevented 280,000 h of potential power outages [51]. However, reverting to 4 G would result in a temporarily smaller bandwidth and slower signal. This would mean that 5G-enabled features would not operate at optimal speeds or that not all smart devices could be functional at the same time. In order to prepare for a situation like this, utilities are recommended to identify and prioritize the features that are essential to continue running on the reduced bandwidth, while disabling others until 5 G service can be restored.

3.3.3.8. Cyberattack risks. Nearly all power outages in the past have been due to damages to or vandalism of the distribution system [52], rather than at the power generation or transmission level. Power outages cause an estimated $8851 in financial losses per minute of outage [52]. Because of the distributed nature of the power distribution system's infrastructure, physical security of any new infrastructure added is essential for preventing significant economic consequences. With increased edge computing with 5 G, cybersecurity of edge devices is also essential.

In March 2019, a cyberattack interrupted communication between the power grid control center and the network, temporarily preventing operators from monitoring the network across California, Utah, and Wyoming. In December 2019, a ransomware attack targeting power grids in the U.S., Japan, and Europe disrupted operations, causing a decrease in productivity and revenue [56]. These events show the possible consequences of cyberattacks targeting a smart power grid. Although between 2014 and 2018, only four cybersecurity incidents were reported on the U.S. power grid [52], the introduction of 5 G and more automated features can increase access points for such attacks. Increased physical access to components of a power grid create opportunities for cyber-physical attacks, which exploit both hard- and software vulnerabilities simultaneously, resulting in reduced quality of service and economic damages [57].

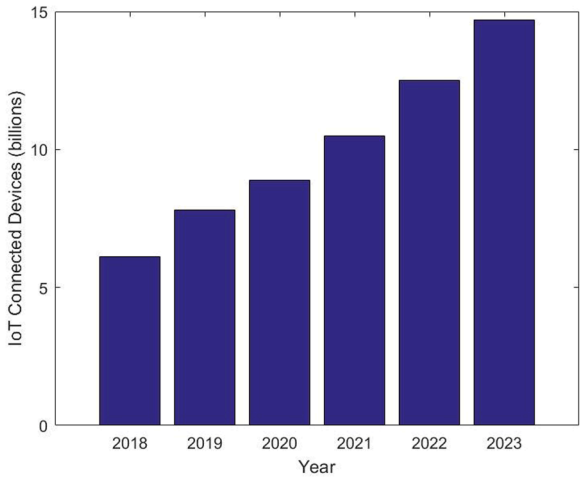

Fig. 3. Number of global connected IoT devices.

The number of connected IoT devices to the grid is projected to steadily increase, as shown in Fig. 3, with billions of devices already connected worldwide [58].

In particular, smart appliances utilizing 5 G capabilities may pose a substantial risk to the power grid. Botnet attacks using appliances such as smart refrigerators, smart air conditioners, etc., can disrupt the power grid by overloading it [49,59]. Botnet attacks occur when hackers gain control of large numbers of smart devices. Smart appliances are often easy targets because they have few cybersecurity features. An attacker can cause all the devices in the botnet to maximize their energy consumption simultaneously, overloading the power grid. Given the large and growing number of smart devices connected and online, an attack like this is very realistic, and a small perturbation can lead to significant effects. For example, even a 1% surge in power demand in the state of California can overload most of the state's grid [51]. Because IoT devices are developed by many different entities, security features vary widely. The role of electricity providers in preventing such attacks is to maximize cybersecurity measures at the edges of the network and limit the access from end-user devices such as smart appliances and meters to other parts of the grid. Additionally, optimizing the power usage of the connected devices can make it harder to overload the power grid. Humayun et al. present a framework for maximizing energy efficiency in a 5G-enabled smart grid while also maintaining the privacy of the connected devices' data [60]. While this may not prevent botnet attacks entirely, it can prevent some accidental power grid overloading, which can have the same impacts as a botnet attack outage.

3.3.3.9. Privacy risks. Smart energy meters pose similar privacy risks as smart water meters. The installation of meters in neighborhoods creates more physical access points for attackers. Meters gather sensitive information about households' hourly energy consumption, which can be used to plan targeted break-ins when residents are away. Customers are also vulnerable to phishing attacks in which malicious actors attempt to gain access to customer accounts containing data about energy consumption as well as resident names, addresses, and billing information. Such phishing and other social engineering attacks to gain access to personal information is a growing concern [61]. Providing customers information about how to identify such social engineering attacks and limiting the amount of data that can be accessed through a customer account can minimize these risks.

3.3.4. Smart gas and oil

Oil and gas provide 65% of the nation's energy [52]. With 135 oil refineries in the U.S operating at almost full capacity, there is little backup capacity in the case of a large-scale service interruption. Any refinery downtime would result in a spike in oil prices, resulting in widespread economic consequences on downstream dependent sectors [52]. The spike in U.S. oil prices in March 2022, for example, resulted in increased prices of gasoline, ride-sharing services, public transit, airplane tickets, heating bills, and the transportation of virtually all goods, the costs of which were passed down to consumers in the form of increased consumer prices [62]. Oil sector disruptions can cascade into other industries as well. For example, because plastic is partially derived from oil, disruptions in the oil sector can lead to surges in the cost of plastic production, intensifying the rise in consumer good prices [62].

Natural gas systems provide 37% of the nation's electricity [63]. It is expected that natural gas pipeline shutdowns would cause more severe effects than oil pipeline shutdowns because power plants typically have backup storages of gasoline, but not of natural gas, as natural gas is more difficult to store. Additionally, the power grid is largely dependent on natural gas availability. Despite this, the natural gas industry has few cybersecurity standards and regulations. The new risks that 5 G will introduce are, therefore, critical to address for these systems.

Oil and gas networks are described together here, as both are pipeline infrastructure with similar applications of 5 G technology. 5G-enabled features such as real-time monitoring of facilities and earlier detection of components requiring service will result in less unplanned shutdowns for maintenance. The resulting increase in efficiency can reduce maintenance costs by 10% [64]. Another application of 5 G in the smart gas and oil industry is enabling real-time communication with field workers to guide technicians through specialized repairs [65]. The automation of dangerous procedures such as drilling processes also seeks to improve safety conditions for workers [64].

3.3.4.10. Risks during transition to 5 G and risks in the case of a 5 G network disruption. Because the 5 G rollout will be focused on densely populated areas at first, there will be a lack of or delay in the availability of 5 G service in rural areas, where many oil and gas companies are located [65]. Oil and gas infrastructure is spread over a wide geographic areas. Therefore, 5 G may also be available only in some parts of the network, making it difficult to implement many of the envisioned smart gas and oil network features in the near future. The transition points between 5G-enabled and non-5G-enabled assets will also need to be considered.

In addition, the oil and gas industry is highly regulated. Although 5 G can be used to automate dangerous activities, creating safer working conditions for workers, international safety laws and regulations during drilling make it difficult to explore use of 5 G in many contexts [64]. Implementing these new 5G-enabled features in smart oil and gas systems is expected to take longer than in other applications.

During a 5 G network disruption, networks in this sector can expect a temporary reduction in the efficiency enabled by the smart features. Depending on the duration of the outage, this may result in economic losses as more steps of the oil and gas production and transmission process need to be done manually, and an increase in maintenance and operation costs. If the network is able to adapt quickly, however, functionality can still be maintained. Planning for a network disruption involves prioritizing vital systems that need to remain up and running on the reduced bandwidth provided by existing 4 G or WiFi signal.

In other applications, such as 5G-enabled automation of drilling processes, network disruptions have the potential for more severe consequences, and can result in environmental damage or harm to employees in the vicinity [66]. In order to safely implement automated procedures like this, it is essential to have backup plans and safety measures that can be implemented virtually instantaneously to prevent harm to workers or the environment.

3.3.4.11. Cyberattack risks. Based on past cybersecurity incidents, targeted, politically motivated attacks present a substantial security risk to smart oil networks. Natural gas networks have experienced fewer cyberattacks; however, the similarity in their operations means they are also susceptible. In 2012, a cyberattack targeting an oil company resulted in data deleted from 30,000 computers and damage to nearly 75% of the company's IT infrastructure [67]. Disruptions in service caused by this attack lasted several weeks. In another incident in 2017, malware interfered with safety mechanisms at an oil refinery plant [67]. Though this resulted in no severe impacts due to early detection, it could have led to plant shutdowns, safety hazards for employees, and environmental damage [68]. U.S. officials have stated that the same group responsible for the 2017 attack have made similar attempts targeting a U.S. oil company and that, as of early 2022, the group remains a threat to U.S. infrastructure [69]. Continued collaboration between government and private companies to monitor known hackers and groups who may target CI systems can help companies to prepare for specific attacks that are suspected.

Ransomware attacks are also a notable type of cyberattack affecting the oil industry. It is estimated that 28% of oil companies and 25% of natural gas companies are "highly likely" to experience a ransomware attack [70]. The existing minimal security measures throughout the network would allow malicious actors widespread access once in the

network [70]. This vulnerability highlights the need for a zero-trust model, a security model that assumes that even if a user has gained access to the network, they are not trusted with all of the network's information and controls. In a zero-trust approach, checkpoints throughout the network repeatedly authorize access to the user at various stages [71]. A zero-trust model can limit the actions of a hacker that successfully gains access through stolen employee credentials, physical vulnerabilities, etc., and minimizes the likelihood of severe consequences. While all smart CI systems can benefit from such an approach, the zero-trust model is especially valuable for the smart oil and gas sector because of the higher likelihood of sophisticated attacks, the severity of potential impacts, and the current lack of authorization checkpoints within the network.

3.3.4.12. Privacy risks. One of the most widely publicized cybersecurity attacks on CI occurred in May 2021. A hacking group gained access to Colonial Pipeline's system using a stolen ex-employee's password and held nearly 100 GB of data for ransom from the company. The group also disrupted the company's billing infrastructure, making them unable to bill customers properly. The attack caused the pipeline to shut down for the first time in its 57-year lifetime. The pipeline remained shut down for six days, causing gas shortages and a sharp increase in gas prices as people began panic-buying gasoline. In the end, the company paid the $4.4 million ransom payment [74]. As shown by this event, the economic and social consequences of the hacking of the network can be severe. 5 G will worsen the potential effects of such attacks by increasing automation throughout the network and thereby reducing the involvement and oversight of employees. Protecting employee credentials by changing them regularly and removing access as soon as an employee has left the company are simple steps that can be implemented to minimize such vulnerabilities. Additionally, adding manual checkpoints throughout, where employees ensure that everything is running as expected, can minimize the impacts of cyberattacks and malfunctions.

3.4. Common themes and risk mitigation recommendations across sectors

The previous sections describe specific risks associated with 5 G for varying smart infrastructure systems, previous historical events that may indicate future risks and attacks, and mitigation recommendations for the range of risks identified. This section looks across sectors to identify common themes and risk mitigation recommendations.

The most prevalent theme across the CI sectors is the increased number of threat vectors that 5 G brings. Infrastructure systems are by nature large, complex networks with many interconnected and interacting components. Such a network is more challenging to secure because each new component or device brings potential new risks in terms of both physical and cybersecurity vulnerabilities. Fragmented ownership throughout a highly interdependent network adds an additional layer of difficulty. Because of this, collaboration between government organizations, investors, operators, and manufacturers of smart devices is crucial for minimizing security gaps across a single CI network. Consistent reporting of known cyberattacks is also valuable to help other infrastructure owners and operators prepare for similar attacks.

Another theme is the importance of early detection of unusual activity. In many of the real-world historical cases described, the most severe consequences were prevented by rapid intervention by employees. As 5 G allows more of the maintenance and operation tasks for a network to be automated, the role of employees will shift towards maintaining a careful watch over the system, prepared to intervene in the case of a malfunction or cyberattack. Successfully making this transition in job responsibilities will require a shift in workforce development and training. Creating robust backup plans so that a system can switch to manual or 4G-based operations in the case of a 5 G outage is another common theme across sectors. Finally, as 5 G technologies and connected devices continue to be developed, new risks will continue to emerge. Therefore, it is important that cybersecurity standards are agile and able to evolve and adapt to meet the needs of a changing risk landscape. Fig. 4 summarizes the major risk themes identified across the smart CI systems analyzed and corresponding risk mitigation recommendations.

To illustrate commonalities and differences in 5 G risks across CI sectors, Fig. 5 shows the common risk themes across the four sectors analyzed. Fig. 5 shows that while the majority of the major risk themes identified apply to all four sectors investigated in this paper, some themes are relevant to only some of the sectors. This highlights that because 5 G will be utilized differently by each sector and each network has unique characteristics, it is essential for CI system owners and operators to make individual assessments of their systems to fully evaluate their risk profiles and take corresponding actions for risk mitigation.

4. Conclusions

The introduction of 5 G technology presents new threats not only to the telecommunications network but also to CI systems that will rely on it to provide vital community resources including mobility, water, power, and oil and gas. The development of 5 G technology creates many more opportunities than previously existed for automation in smart critical infrastructure. Implementing these features requires increased interconnection between the telecommunications network and critical infrastructure networks. Additionally, the installation of many new connected devices such as sensors, smart meters, and smart roadside infrastructure creates more entrance points into the CI network that must be secured both physically and digitally. Lastly, these devices collect more private information than has been collected previously (e.g., hourly water usage, vehicle location, vehicle movement direction, etc.). These large-scale changes mean that security risks affecting the telecommunications network that were not previously the concern of CI operators are now relevant to them, and new privacy risks emerge that are not necessarily inherent to 5 G but brought on by the technology that 5 G enables. This paper investigates how 5 G and the increased number of IoT devices that are needed for 5G-enabled smart features in these networks will change the risk landscape for four major CI sectors, covering risks during the rollout of and transition to 5 G, risks in the case of a 5 G network disruption, cyberattack risks, and privacy risks for each sector. Importantly, this paper also assesses specific challenges that the sectors may face during the transition period, as 5 G infrastructure is built out and more smart features become available.

As 5 G technologies continue to be developed and deployed, there are growing risks associated with 5 G for CI, as well as existing risks that persist after the introduction of 5G-enabled smart features. Though past outages and attacks provide some information about what can be expected, the risk landscape will become clearer as 5 G technologies are implemented. The purpose of early risk assessment as described in this paper is to enable early risk mitigation. At the same time, with developing technologies, it is necessary for cybersecurity, 5 G, and technology standards to evolve constantly as more becomes known. In cases where policy updates cannot be made quickly enough, collaboration between researchers and industry best practices should encourage CI networks of all sizes to keep up-to-date with the latest cybersecurity recommendations. This paper provides a detailed assessment of the emerging risks associated with the transition to 5 G, allowing sectors to investigate and implement mitigation measures with the identified risk themes in mind to minimize vulnerabilities and increase the reliability and resilience of CI systems.

Data availability statement

All data, models, and code generated or used during the study appear in the submitted article.

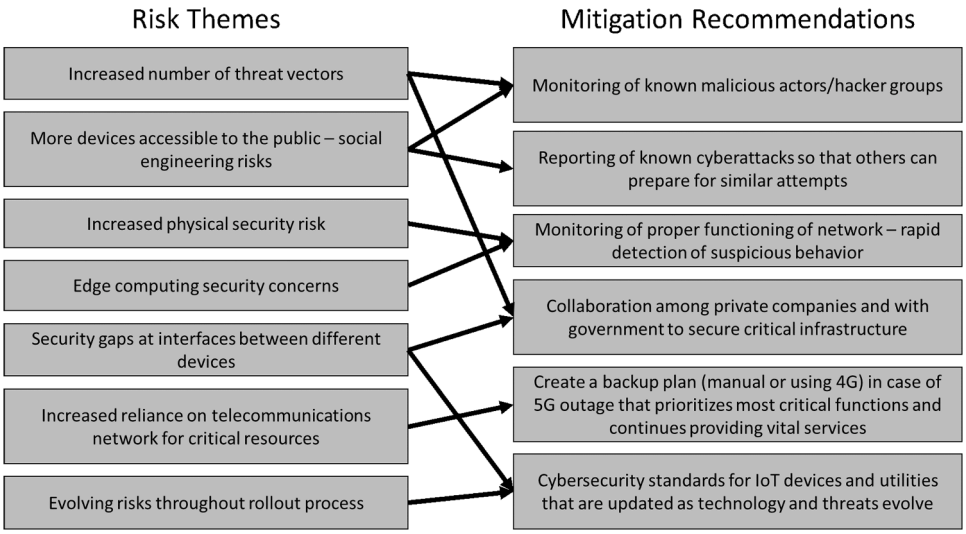

Fig. 4. Risk themes across critical infrastructure sectors and corresponding mitigation recommendations.

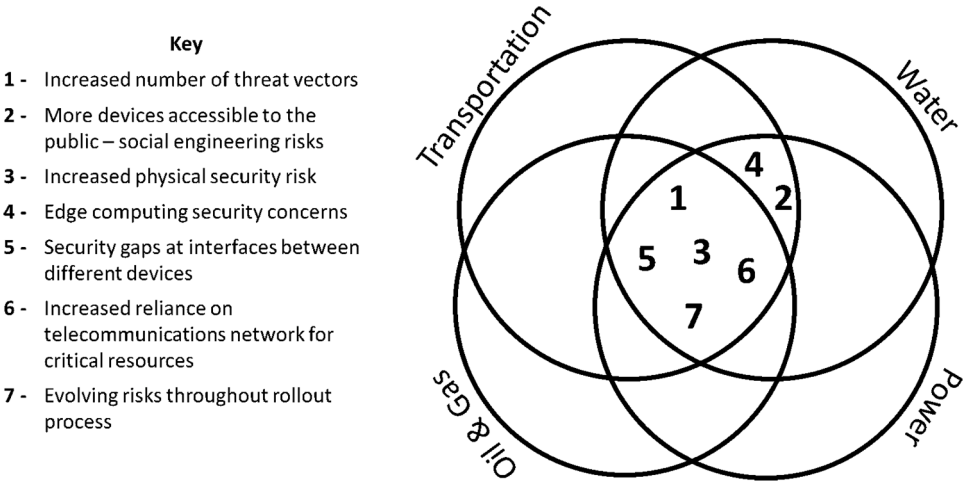

Fig. 5. Common risk themes across critical infrastructure sectors.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Funding

This material is based upon work funded by the U.S. Department of Homeland Security under Cooperative Agreement No. 2015-ST-061-CIRC01–03.

Acknowledgements

Support for this work from the U.S. Department of Homeland Security under Cooperative Agreement No. 2015-ST-061-CIRC01–03 is acknowledged.

References

[1] White House. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[2] I. Tien, Recommendations for Investing in Infrastructure at the Intersection of Resilience, Sustainability, and Equity, ASCE J. Infrastruct. Syst. 28 (2) (2022). June.
[3] G. Pescaroli, D. Alexander, Critical infrastructure, panarchies and the vulnerability paths of cascading disasters, Nat. Hazards 82 (1) (2016) 175–192, https://doi.org/10.1007/s11069-016-2186-3.
[4] C. Johansen, I. Tien, Probabilistic multi-scale modeling of interdependencies between critical infrastructure systems for resilience, Sustain. Resilient Infrastruct. 3 (1) (2018) 1–15.
[5] Berkeley, A.R., III, Wallace, M., & National Infrastructure Advisory Council. (2010). A framework for establishing critical infrastructure resilience goals. https://www.cisa.gov/sites/default/files/publications/niac-framework-establishing-resilience-goals-final-report-10-19-10-508.pdf.
[6] C. Johansen, J. Horney, I. Tien, Metrics for evaluating and improving community resilience, ASCE J. Infrastruct. Syst. 23 (2) (2017). June.
[7] C. Applegate, I. Tien, Framework for probabilistic vulnerability analysis of interdependent infrastructure systems, ASCE J. Comput. Civ. Eng. 33 (1) (2019). January.
[8] W. Suo, L. Wang, J. Li, Probabilistic risk assessment for interdependent critical infrastructures: a scenario-driven dynamic stochastic model, Reliab. Eng. Syst. Saf. 214 (2021), 107730, https://doi.org/10.1016/j.ress.2021.107730.
[9] A. Kim, J. Oh, K. Kwon, K. Lee, Consider the consequences: a risk assessment approach for industrial control systems, Secur. Commun. Netw. 2022 (2022), e3455647, https://doi.org/10.1155/2022/3455647.

[10] A. Hassanzadeh, et al., A review of cybersecurity incidents in the water sector, J. Environ. Eng. 146 (5) (2020), 03120003, https://doi.org/10.1061/(asce)ee.1943-7870.0001686.
[11] Huq, N., et al. TrendLans, 2018, Cyberattacks against intelligent transportation systems, https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf. Accessed 11 Mar. 2022.
[12] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks, Int. J. Crit. Infrastruct. Prot. 25 (2019) 36–49, https://doi.org/10.1016/j.ijcip.2019.01.001.
[13] Cybersecurity and Infrastructure Security Agency (CISA) (2021). "Potential Threat vectors to 5G infrastructure" https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf.
[14] A. Ziani, A. Medouri, A survey of security and privacy for 5G networks, M. B Ahmed, S. Mellouli, L. Braganca, B. A Abdelhakim, & K. A. Bernadetta. Emerging Trends in ICT For Sustainable Development, Springer International Publishing, 2021, pp. 201–208, https://doi.org/10.1007/978-3-030-53440-0_22.
[15] W. Mazurczyk, P. Bisson, R.P. Jover, K. Nakao, K. Cabaj, Challenges and novel solutions for 5G network security, privacy and trust, IEEE Wirel. Commun. 27 (4) (2020) 6–7, https://doi.org/10.1109/MWC.2020.9170261.
[16] R. Borgaonkar, et al., Improving smart grid security through 5G enabled IOT and edge computing, Concurr. Comput. Pract. Exp. 33 (18) (2021) 2021, https://doi.org/10.1002/cpe.6466.
[17] C. Lai, R. Lu, D. Zheng, X. Shen, Security and privacy challenges in 5G-enabled vehicular networks, IEEE Netw. 34 (2) (2020) 37–45, https://doi.org/10.1109/MNET.001.1900220.
[18] B. Yang, Z. Yu, J. Lan, R. Zhang, J. Zhou, W. Hong, Digital beamforming-based massive 9 MIMO transceiver for 5G millimeter-wave communications, IEEE Trans. 10 Microwave Theory Tech. 7 (66) (2018) 3403–3418.
[19] S. Alam, S.T. Siddiqui, A. Ahmad, R. Ahmad, M. Shuaib, Internet of Things (IoT) 4 enabling technologies, requirements, and security challenges, Kolhe M., Tiwari S., Trivedi M., Mishra K.. Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, Springer, Singapore, 2020, 94ASCE. Drinking Water - 2021 Infrastructure Report Card. American Society of Civil Engineers, 2021, https://infrastructurereportcard.org/wp-content/uploads/2020/12/Drinking-Water-2021.pdf.
[20] M.A. Lema, A. Laya, T. Mahmoodi, M. Cuevas, J. Sachs, J. Markendahl, M. Dohler, Business case and technology analysis for 5G low latency applications, IEEE Access 5 (2017) 5917–5935, https://doi.org/10.1109/ACCESS.2017.2685687.
[21] C. Bockelmann, N. Pratas, H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski, A. Dekorsy, Massive machine-type communications in 5 g: physical and MAC-layer solutions, IEEE Commun. Mag. 54 (9) (2016) 59–65, https://doi.org/10.1109/MCOM.2016.7565189.
[22] J. Vestin, A. Kassler, Low frequency assist for mmWave backhaul-the case for SDN resiliency mechanisms, in: Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), 2017, pp. 205–210.
[23] T-Mobile. (2022). Why mid-band matters for 5G. T-Mobile for Business. https://www.t-mobile.com/business/trends-insights/5g/why-mid-band-5g-matters.
[24] Nokia. (2022). 5G spectrum bands explained — Low, mid and high band. Retrieved January 2, 2023, from https://www.nokia.com/networks/insights/spectrum-bands-5g-world/.
[25] E. Lagunas, C.G. Tsinos, S.K. Sharma, S. Chatzinotas, 5G cellular and fixed satellite service spectrum coexistence in C-band, IEEE Access 8 (2020) 72078–72094, https://doi.org/10.1109/ACCESS.2020.298501.
[26] U.S Department of Transportation, Federal aviation administration, FAA airworthiness directive: the boeing company airplanes, Feb. 24, 2022, https://public-inspection.federalregister.gov/2022-03967.pdf.
[27] L. Li, D. Wang, X. Niu, Y. Chai, L. Chen, L. He, X. Wu, F. Zheng, T. Cui, X. You, mmWave communications for 5G: implementation challenges and advances, Sci. China Inf. Sci. 61 (2) (2018), 021301, https://doi.org/10.1007/s11432-017-9262-8.
[28] Verizon. (2020). What frequency is 5G? Verizon News Center. Retrieved January 2, 2023, from https://www.verizon.com/about/our-company/5g/what-frequency-5g.
[29] M. Höyhtyä, J. Huusko, M. Kiviranta, K. Solberg, J. Rokka, Connectivity for autonomous ships: architecture, use cases, and research challenges, in: Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), 2017, pp. 345–350, https://doi.org/10.1109/ICTC.2017.8191000.
[30] S.F. Chou, T.C. Chiu, Y.J. Yu, A.C. Pang, Mobile small cell deployment for next generation cellular networks, in: Proceedings of the IEEE Global Communications Conference, 2014, pp. 4852–4857.
[31] A. Nordrum, K. Clark, 5G bytes: small cells explained, IEEE Spectr. 2 (2017). August 19, https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained.
[32] TechTarget Inc & T-Mobile. (2020). A phased approach to effective 5G implementations. Retrieved January 2, 2023, from https://www.t-mobile.com/content/dam/tfb/pdf/TFB_TechTarget-whitepaper_Phased-Approach-to-5G-Implementation.pdf?icid=TFB_TMO_P_20CONTENT_MHBX1AU89ENJ84J623702.
[33] W. Wu, Q. Zhang, H.J. Wang, Edge computing security protection from the perspective of classified protection of cybersecurity, in: Proceedings of the 6th International Conference on Information Science and Control Engineering (ICISCE), 2019, pp. 278–281, https://doi.org/10.1109/ICISCE48695.2019.00062.
[34] Jover & Marojevic, 2019.
[35] AT&T. (n.d.). AT&T Rolls Out 5G+ Across the U.S. Retrieved January 2, 2023, from https://about.att.com/pages/5g-plus.html.
[36] GSMA. 2019. "Connecting Vehicles Today and in the 5G Era With C-V2X." https://www.gsma.com/iot/wp-content/uploads/2019/08/Connecting-Vehicles-Today-and-in-the-5G-Era-with-C-V2X.pdf.
[37] E. Aria, J. Olstam, C. Schwietering, Investigation of automated vehicle effects on driver's behavior and traffic performance, Transp. Res. Procedia 15 (2016) 761–770, https://doi.org/10.1016/j.trpro.2016.06.063.
[38] European Telecommunications Standards Institute (ETSI), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service (102 637-2 V1.2.1 (2011-03)), European Telecommunications Standards Institute, 2011. Retrieved January 2, 2023, from, https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf.
[39] C. Oham, R.A. Michelin, R. Jurdak, S.S. Kanhere, S. Jha, B-FERL: blockchain based framework for securing smart vehicles, Inf. Process Manag. 58 (1) (2021), 102426, https://doi.org/10.1016/j.ipm.2020.102426.
[40] P. Vargas, I. Tien, Methodology to quantitatively assess impacts of 5G telecommunications cybersecurity risk scenarios on dependent connected urban transportation systems, ASCE-ASME J. Risk Uncertain. Eng. Syst. Part A Civ. Eng. 8 (2) (2022), 04022004, https://doi.org/10.1061/AJRUA6.0001220.
[41] Y. Lalle, M. Fourati, L.C. Fourati, J.P. Barraca, Communication technologies for Smart Water Grid applications: overview, opportunities, and research directions, Comput. Netw. 190 (2021), 107940, https://doi.org/10.1016/j.comnet.2021.107940.
[42] M.N. Adams, O. Jokonya, An investigation of smart water meter adoption factors at universities, Procedia Comput. Sci. 196 (2022) 324–331, https://doi.org/10.1016/j.procs.2021.12.020.
[43] C. Feng, Y. Wang, Q. Chen, Y. Ding, G. Strbac, C. Kang, Smart grid encounters edge computing: opportunities and applications, Adv. Appl. Energy 1 (2021), 100006, https://doi.org/10.1016/j.adapen.2020.100006.
[44] W. Shi, et al., Edge computing: vision and challenges, IEEE Internet of Things Journal 3 (5) (2016) 637–646, https://doi.org/10.1109/jiot.2016.2579198.
[45] P.V. Osdol, FBI Investigating Hacking Threats at Pennsylvania Water Systems, Pittsburgh's Action News, 2021, 26 June, https://www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504.
[46] Ropek, L. "Ransomware Hackers Reportedly Targeted 3U.S. Water Facilities in 2021." Gizmodo, Gizmodo, 18 Oct. 2021, https://gizmodo.com/ransomware-hackers-reportedly-targeted-3-different-u-s-1847874992.
[47] ASCE, Drinking Water - 2021 Infrastructure Report Card, American Society of Civil Engineers, 2021. https://infrastructurereportcard.org/wp-content/uploads/2020/12/Drinking-Water-2021.pdf.
[48] KPMG. (2019). Managing IoT risk in power and utilities. Retrieved December 30, 2022, from https://assets.kpmg/content/dam/kpmg/us/pdf/2019/07/managing-iot-risks-in-power-and-utilities.pdf.
[49] A. Israr, et al., Renewable energy powered sustainable 5G network infrastructure: opportunities, challenges and perspectives, J. Netw. Comput. Appl. 175 (2021), https://doi.org/10.1016/j.jnca.2020.102910, 1 Feb.
[50] Eaton, 2018, Blackout Tracker, United States Annual Report 2018, https://www.eaton.com/explore/c/us-blackout-tracker-1-2?x=NzOhds. Accessed 11 Mar. 2022.
[51] ASCE, Energy - 2021 Infrastructure Report Card, American Society of Civil Engineers, 2021 b, https://infrastructurereportcard.org/wp-content/uploads/2020/12/Energy-2021.pdf.
[52] J.P. Mohan, N. Sugunaraj, P. Ranganathan, Cyber security threats for 5G networks, in: Proceedings of the IEEE International Conference on Electro Information Technology (EIT), 2022, pp. 446–454, https://doi.org/10.1109/eIT53891.2022.9813965.
[53] E. Lee, Y.D. Seo, S.R. Oh, Y.G. Kim, A Survey on standards for interoperability and security in the Internet of Things, IEEE Commun. Surv. Tutor. 23 (2) (2021) 1020–1047, https://doi.org/10.1109/COMST.2021.3067354.
[54] T. Alladi, V. Chamola, B. Sikdar, K.K.R. Choo, Consumer IoT: security vulnerability case studies and solutions, IEEE Consum. Electr. Mag. 9 (2) (2020) 17–25, https://doi.org/10.1109/MCE.2019.2953740.
[55] United States Government Accountability Office. (2021). DOE needs to ensure its plans fully address risks to distribution systems. Retrieved January 2, 2023, from https://www.gao.gov/assets/gao-21-81.pdf.
[56] P.K. Jena, S. Ghosh, E. Koley, Design of a coordinated cyber-physical attack in IoT based smart grid under limited intruder accessibility, Int. J. Crit. Infrastruct. Prot. 35 (2021), 100484, https://doi.org/10.1016/j.ijcip.2021.100484.
[57] Cisco, "Annual Internet Report (2018-2023) White Paper," 19 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet20report/white-paper-c11-741490.html, updated March 2020.
[58] Y. Guo, L. Yan, Z. Chen, Z. Zhao, D. Bai, Z. Ding, Y. He, Defending 5G IoT terminals in electrical power communication and information system against cyber threats, in: Proceedings of the IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), 2021, pp. 1–5, https://doi.org/10.1109/EI252483.2021.9712987.
[59] M. Humayun, N. Jhanjhi, M. Alruwaili, S.S. Amalathas, V. Balasubramanian, B. Selvaraj, Privacy protection and energy optimization for 5G-aided industrial Internet of Things, IEEE Access 8 (2020) 183665–183677, https://doi.org/10.1109/ACCESS.2020.3028764.
[60] D. Faquir, et al., Cybersecurity in smart grids, challenges and solutions, AIMS Electron. Electr. Eng. 5 (1) (2021) 24–37, https://doi.org/10.3934/electreng.2021002.
[61] Ballentine, C. (2022, March 21). It's not just gas: surging oil prices are making more things expensive. Bloomberg.Com. https://www.bloomberg.com/news/articles/2022-03-21/oil-inflation-is-raising-costs-for-uber-rides-housing-groceries-and-vacations.

[62] U.S. Energy Information Administration (EIA). (2022). Use of natural gas. Retrieved November 30, 2022, from https://www.eia.gov/energyexplained/natural-gas/use-of-natural-gas.php.
[63] F. Grijpink, et al., How Tapping Connectivity in Oil and Gas Can Fuel Higher Performance, McKinsey & Company, McKinsey & TCompany, 2020, 6 Nov. https://www.mckinsey.com/industries/oil-and-gas/our-insights/how-tapping-connectivity-in-oil-and-gas-can-fuel-higher-performance.
[64] J. Fritz, N. Clark, 5G and edge computing in oil and gas." Perspectives, Deloitte (2021), 30 July, https://www2.deloitte.com/us/en/pages/consulting/articles/5g-in-oil-and-gas.html.
[65] P. Ciepiela, How digitalization in oil and gas is creating security risks, Ernst Young (EY) (2019), 29 Apr, https://www.ey.com/en_us/oil-gas/how-digitalization-in-oil-and-gas-is-creating-security-risks.
[66] Khan, W., & Khan, K. (2019). Advanced persistent threats through industrial iot on oil and gas industry. 2019, 1–15.
[67] Dragos Inc, 2017, Trisis Malware - Analysis of Safety System Targeted Malware, https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf. Accessed 11 Mar. 2022.
[68] A. Greenberg, Feds allege destructive russian hackers targeted US refineries, Wired (2022). Retrieved July 6from, https://www.wired.com/story/triton-berserk-bear-russian-hackers-doj-indictment/.
[69] Kite B. (2021). The 2021 ransomware risk pulse: energy sector. Retrieved November 30, 2022, from https://blackkite.com/whitepaper/the-2021-ransomware-risk-pulse-energy-sector/.
[70] Microsoft. (2021). Evolving zero trust. Retrieved December 27, 2022, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT.
[71] Turton, W., & Mehrotra, K. (2021, June 4). Hackers breached colonial pipeline using compromised password. Bloomberg.Com. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.