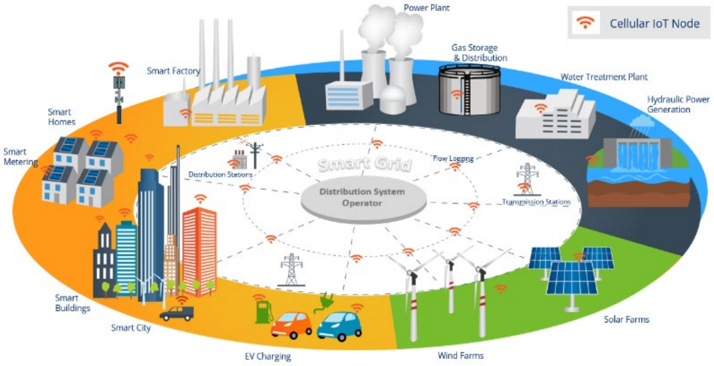
Critical Internet of Things

Introduction

In today's rapidly evolving world, the concept of "smart" has infiltrated nearly every aspect of our lives, revolutionizing our homes, workplaces, and even the transportation systems we rely on. This digital transformation is powered by the Internet of Things (IoT), a network of interconnected devices that gather and exchange data to optimize various processes. One well-known application of IoT is the widespread adoption of Smart Meters, driven by governments worldwide to enhance energy systems.

Smart meters, found in electricity, gas, and water utilities, offer individuals the ability to monitor their resource consumption and usage patterns in real-time. By equipping people with this data, they can make informed decisions to reduce energy usage, save money, and contribute to environmental conservation. Beyond individual benefits, smart meters also play a crucial role in providing critical data about the "quality" of supply at each endpoint. This valuable information is fed into a broader grid management infrastructure, known as the smart grid, which continuously monitors the flow of gas, electricity, and water in a complex and interconnected system.

The need for a smart grid arises from the fact that traditional infrastructures were not designed to meet the demands of modern energy demands, such as the increasing use of Electric Vehicles (EVs) and the integration of alternative green energy resources. The smart grid serves multiple purposes - it ensures that the available power is distributed appropriately when significant energy consumers are operating and continuously adjusts to incorporate clean energy sources from distributed resources.



To achieve this, numerous industrial equipment containing sensors and actuators are deployed throughout the grid. These devices offer real-time insights into the grid's performance and efficiency, transforming it into a vast, single machine that can be remotely tuned and balanced for optimal functionality. The deployment of internet-connected sensors all over the grid provides grid managers with essential insights into the dynamic behavior of their infrastructure.

Without this complex network of internet connected sensors providing the insights to perform load balancing operations we would suffer severe blackouts as the grid would become unstable, hence the connectivity network becomes as vital as the asset it monitors. The internet-connected industrial assets form the backbone of this smart grid, and cellular communication plays a central role in enabling the clean energy transition. Leveraging the existing mobile phone infrastructure, **cellular modules** facilitate seamless interconnection within the **Critical Internet of Industrial Things**.

Buried within the intricacies of the industrial apparatus, these cellular modules provide the crucial link to mobile phone networks, serving as the spine that keeps the communication network running smoothly. In essence, they are instrumental in ensuring that the smart grid functions efficiently, enabling the successful transition towards cleaner energy sources.

Cellular Communication in Critical Industry

Cellular connectivity and cellular modules play a pivotal role in transforming various industries, making smart technologies a reality. Whilst one prime example is the smart grid, which efficiently manages the flow of energy, water, and sewage, ensuring smooth operations for utilities, the significance of cellular modules extends far beyond utilities. Cellular modules connect a wealth of critical applications across multiple sectors.

In the healthcare industry, smart hospitals leverage a digital networking infrastructure, interconnecting assets to provide invaluable services and insights previously unattainable. Remote Patient Monitoring, made possible by cellular modules, allows patients to remain free while physicians monitor their vital signs.

Smart factories rely on cellular modules to bridge the gap between the digital and physical worlds, monitoring the entire production process, from supply chain management to manufacturing tools and individual operators' work on the shop floor.

Security applications benefit from internet-connected surveillance cameras, intrusion monitoring systems, and access control, bolstered by cellular connectivity for enhanced efficacy.

Transportation industries employ cellular communications to monitor road and rail networks, ensuring smooth traffic flow from centralized offices.

Agriculture embraces connected sensors in the soil, agricultural machinery, and pesticide spreading processes, enabling data-driven decision-making for optimized yields.

Even in finance, mobile payment systems powered by cellular modules have revolutionized transactions, simplifying payments for consumers.

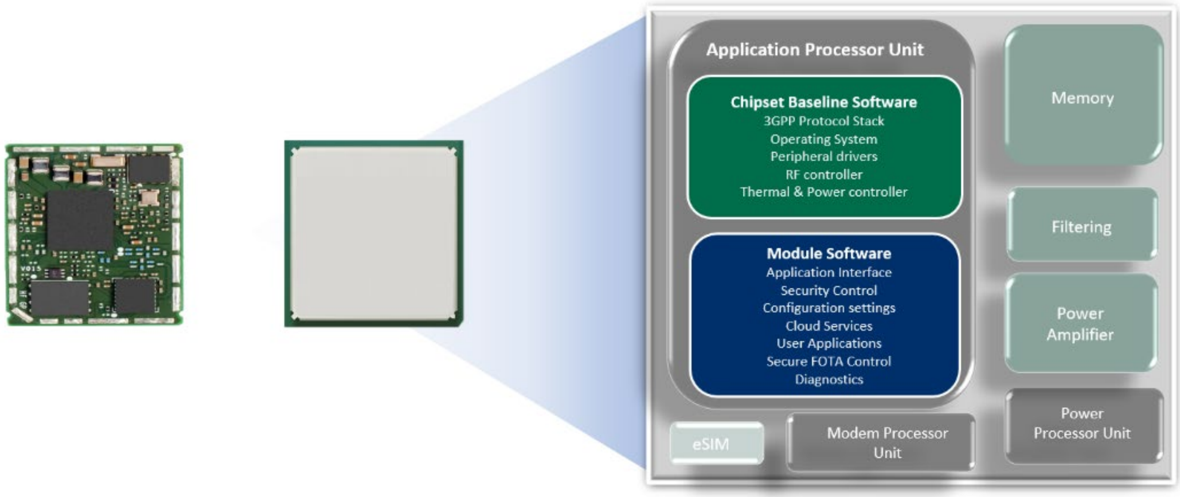
Emergency services have embraced cellular connectivity in vehicles and connected body cameras, improving response times and situational awareness for first responders.

The applications of cellular modules are vast and continue to expand. Almost identical to mobile phones in terms of connectivity services such as internet access, SMS, voice, and location services, when applied to the systems that underpin our daily lives cellular modules become an integral part of critical infrastructure

In essence, these industries and their **essential systems rely on cellular modules** to connect critical equipment to the internet, delivering actionable insights that keep countries' critical operations running smoothly. Cellular modules, acting as the connectivity backbone for machines, provide the necessary link between smart devices and the digital world, enabling industries to thrive and evolve in the communication age.

What is a Cellular Module?

Despite being inconspicuous and often unrecognized, cellular modules play a crucial role as entry and exit points for data, connecting industrial sensors to the cellular network for internet access. While these modules may appear as ordinary chips on a PCB, they are intricate electronic subsystems, running an operating system and potentially millions of lines of firmware code. Essentially, they act as industrial smartphones embedded within critical industrial devices, facilitating the smooth functioning of a country's essential systems.



At the heart of a cellular module lies the baseband chipset, a microprocessor responsible for running the necessary protocol stacks to access cellular networks and various technology standards provided by mobile network operators. They are supplied by established semiconductor companies like Qualcomm or Sony. Integrating such complex functionality directly into devices like smart meters or water pumps is challenging. As a result, equipment manufacturers prefer to opt for modules that handle the complexities of the core chipset.

Beyond the core functionality, modules also encompass other essential peripheral components required to make the core chipset usable, including power and radio components, filtering, and more. Module manufacturers undertake this task of integration, leveraging economies of scale to source components and offer a packaged solution that includes all relevant approvals, such as government-based FCC or CE markings and specific network operator approvals.

However, it's crucial to place complete **trust in the module supplier**, especially concerning the firmware. Inside a module, there exists a substantial amount of code **written by the module manufacturer**. The responsibility lies with the module manufacturer to ensure this critical component is user-friendly for both hardware and software developers while enhancing it with additional features to ensure reliability, security and interoperability with national or global Mobile Network Operators.

It's essential to delve deeper into the trustworthiness of module manufacturers because they have the freedom to shape the capabilities of the device. While the module must fulfill its intended purpose**, it has the potential to do much more**, highlighting the importance of trust in this context.

Essentially, a cellular module is a communication computer, but unlike other products that undergo rigorous approval processes for security, there is no standard "rubber stamp" to guarantee the module's security. Consequently, placing **faith in reputable module manufacturers** becomes paramount to ensure the integrity, reliability, and safety of these critical components in various industrial systems.

Within the module software, the module manufacturer must incorporate remote update functionality. This essential feature allows for bug fixes, performance enhancements, adjustments to mobile network operator settings, or the implementation of security patches.

Similar to a conventional desktop computer, the hardware of the module has limitations and cannot be altered. However, it is the software running on the module that breathes life into it, enabling various functionalities and governing how security and identity are handled. The software serves as the driving force, providing the module with its capabilities and adaptability to evolving requirements

Critical IoT Cyber Security

Undeniably, the rising tide of security concerns in the realm of technology is a cause for alarm. Operational Technology (OT) faces an increasing number of attempted hacks, while IoT systems are coming under greater scrutiny. The vulnerability of critical infrastructure in the wrong hands, especially against the backdrop of geopolitical instability, cannot be overlooked.

Governments worldwide are waking up to the threat posed to critical infrastructure and are taking action to address the security issues related to IoT devices, even down to the individual component level. New bills and proposals are being introduced, aiming to monitor and mitigate vulnerabilities in these systems.

The European Union (EU) has taken a significant step by activating articles in the Radio Equipment Directive. As of Autumn 2024, the new RED-DA (Radio Equipment Directive – Delegated Act) will be enforced for products marketed in the EU, specifically targeting the security of networks, personal and location data, and fraud prevention, such as money transfers. To achieve the coveted CE marking and gain access to the European market, products will need to comply with stringent security measures. This includes safeguarding against ongoing denial-of-service attacks, fortifying attack surfaces, implementing robust access control mechanisms, and ensuring products are free from publicly known vulnerabilities. Additionally, **secure mechanisms for software and firmware updates** are required.

Taking security measures even further, the proposed Cyber Resilience Act, proposed in September 2022, introduces specific requirements for IoT devices. Digital elements are classified based on functionality and intended use. Device makers will be obliged to report and block vulnerabilities in software and firmware.

Furthermore, they must issue **security patches** promptly and at no cost to users, while providing clear explanations about the purpose of the patch.

EU to impose tough rules on 'internet of things' product makers

Companies will face fines of €15mn or 2.5% of turnover if they do not comply with cyber security requirements

The proposed legislation comes a year after Thierry Breton said new rules were needed to counter cyber attacks on the growing internet of things market © Michal Cizek/AFP/Getty Images

Source Financial Times

The NIS2 (Network and Information Security 2) Directive in Europe identifies certain entities, such as those in the Energy, Health, Transport, and Water sectors, as important or essential. Industrial IoT applications falling under these categories would be regarded as class 2 by the Cyber Resilience Act, subjecting them to heightened scrutiny in the process of identifying critical infrastructure.

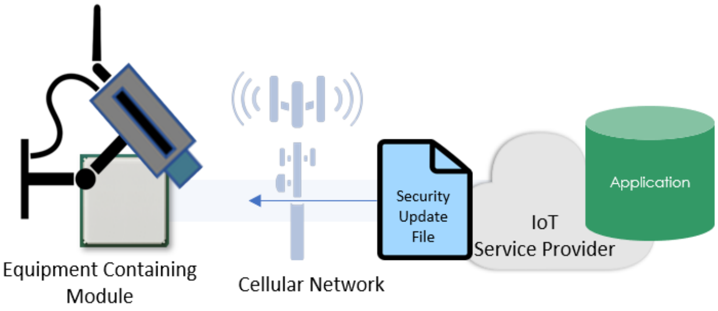
In both cases, manufacturers of these equipment will bear full responsibility for ensuring the overall security of their products. Non-compliance with the prescribed security measures may lead to penalties and legal repercussions.

The growing recognition of the gravity of security risks in technology has spurred governments to take proactive measures. By implementing laws and regulations at various levels, they strive to safeguard critical infrastructure and protect users from potential cyber threats.

Maintenance of Critical IoT Equipment

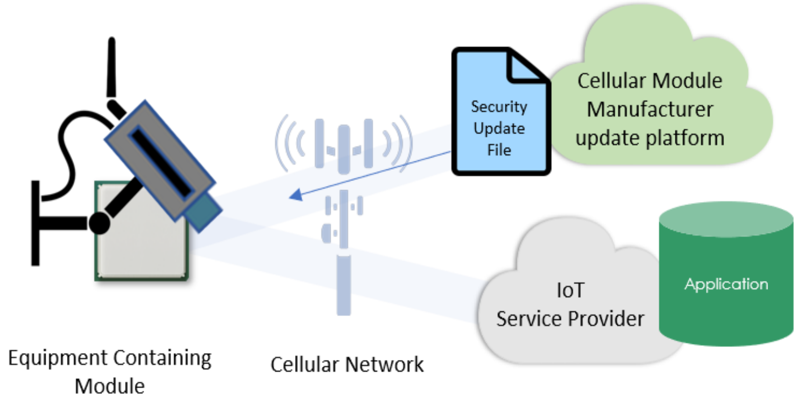
Just like a cell phone may prompt with messages stating that updates will be installed, a similar scenario exists for cellular modules, driven by the same reasons. When it comes to these updates, the process resembles that of a cell phone – while Apple provides updates for your phone, cellular module updates are delivered either directly or indirectly from the module manufacturer. Thus, even after critical equipment is designed, manufactured, installed, and operational, the **reliance on the module manufacturer remains an integral part of the critical infrastructure**. The EU acts, as mentioned earlier, will mandate the requirement to perform these updates.

Let's explore the indirect case first. In this scenario, module manufacturers make encrypted firmware updates available to their customers as files. Customers are responsible for remotely uploading and installing these updates to the modules within their own equipment.



Firmware update Managed by IoT Service Provider

Considering the direct case, which resembles the approach as used by Apple. Due to the scale and complexity of managing vast fleets of equipment, module manufacturers offer a suite of tools to manage update campaigns from their own platforms. This process occurs under the control and agreement of the equipment maker, but it always entails a legitimate communication link between the equipment and the module manufacturer's servers. As a result, **the module manufacturer gains significant visibility** into their customers' fleets of remote equipment, with their update servers forming an integral part of the overall system.


Security Update File
Cellular Module Manufacturer update platform
IoT Service Provider
Application
Equipment Containing Module
Cellular Network

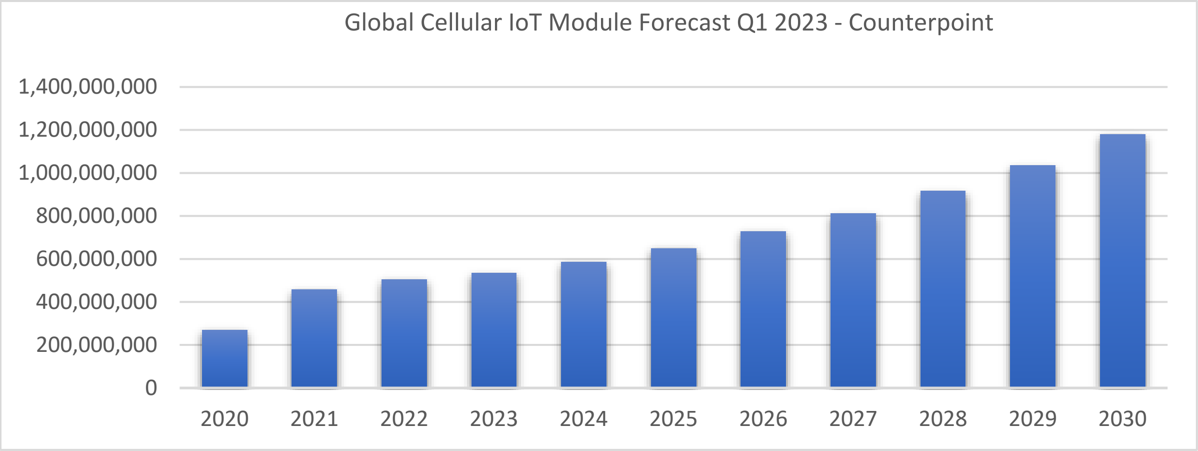
Firmware update Managed by Cellular Module Manufacturer

This distinctive approach sets module manufacturers apart from almost every other component provider in the industry. Their customers, as well as the chain of beneficiaries from IoT systems, continue to rely on the module manufacturer to ensure the ongoing maintenance and security of their products throughout the extended lifespan of industrial equipment.

In essence, the role of the module manufacturer goes beyond merely supplying the component; it extends to supporting customers in keeping their equipment up-to-date and secure. This level of commitment and continuous engagement sets module manufacturers apart as essential partners in the success and longevity of critical industrial infrastructure.

Why Cellular Connectivity for Critical Internet of Things?

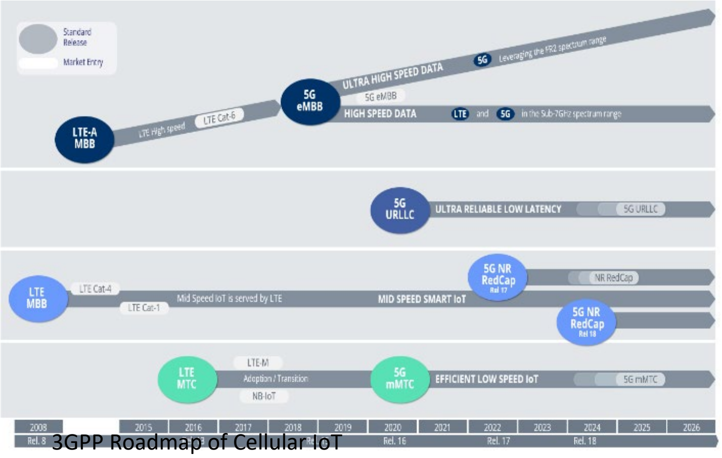
The adoption of cellular communications as a method of connecting machines is experiencing rapid growth. While it is not the only way to connect industrial equipment, cellular technology offers several attractive features that set it apart. Although it comes with a cost, requiring an airtime contract similar to your phone, the numerous advantages of cellular make it an excellent choice for long-term IoT deployments.



One of the key factors that make cellular appealing is its visible roadmap, scale, and global standards. With countless investments from hundreds of operators worldwide, cellular technology provides a robust and widely supported option for connecting IoT devices over extended periods. Moreover, its licensed spectrum and adherence to standards ensure a globally agreed-upon roadmap, guided by the international body 3GPP, with the GSMA representing Network Operators' interests.

3GPP has specifically defined standards tailored for machine communication, evolving from 5G to 6G. Contrary to common perceptions of high-speed broadband technology, 5G encompasses various branches, catering to diverse needs such as very low power consumption, low latency, and ultra-high reliability. This adaptability and scalability make cellular connectivity particularly well-suited for the critical infrastructure needs of the future.

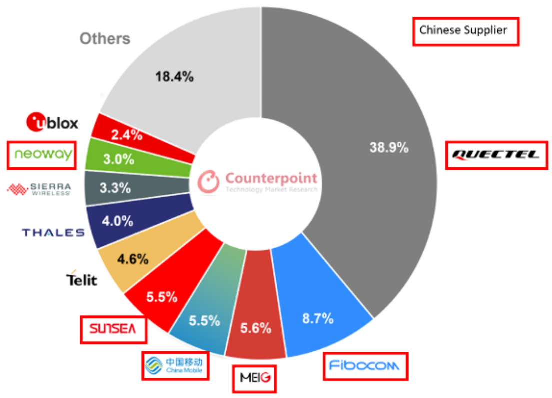
Overall, the combination of cellular technology's established roadmap, global standardization, and support from a vast network of operators makes it a compelling choice for powering long-term IoT deployments, including critical infrastructure. Its evolution into 5G and beyond ensures that cellular will continue to play a vital role in meeting the demands of connected industries for years to come.



3GPP Roadmap of Cellular IoT

The Impact of Chinese Cellular Module Manufacturers

In 1996, Siemens, which has now evolved into Telit Cinterion, introduced the first cellular module to the market. Since then, the industry has seen multiple manufacturers emerge, with various mergers, acquisitions, and consolidations, leading to consistent double-digit growth.



In recent years, Chinese manufacturers have witnessed rapid growth in the electronics industry, even expanding their presence in Europe and North America. Consequently, there are now millions of Chinese cellular modules, or communications computers, embedded within Western industrial equipment. The key reason for their popularity is their irresistibly low price, approximately 60% of what Western players can offer.

According to a report titled "HOW THE CCP SUPPORTS THE CHINESE CELLULAR IoT MODULE SECTOR," written by Charles Parton, a former UK Chinese diplomat and released by analyst OODA Loop, *"In the IoT sector, the party-state ensures that IoT companies receive favourable regulatory treatment, finance at preferential rates through central and regional banking institutions, access to key materials and products (such as semiconductors) at below cost, and other state support. These measures create a favourable and interconnected ecosystem for technology companies working on these strategic technologies."*

IoT is indeed a strategic technology for the Chinese government as set out in their 5 year plan to develop Internet of Things infrastructure.

Despite the cost advantage, concerns about cyber security exist. Governments worldwide have already taken measures against Huawei due to security risks in 5G core equipment. While this issue has garnered high-profile attention due to the company's size and scale, there are millions of Chinese cellular modules dispersed across the infrastructure of Western nations. While data interception and spying are potential risks, it is also technically possible for a module manufacturer to locate, destabilize, or disable remote assets containing their software. The direct method of updating modules makes this process relatively easy.

A notable example occurred in November 2022 when Chinese IoT Module Manufacturer Quectel issued a Product Change Notification (PCN), detailing a new firmware upgrade to prevent modules from working in Russia or Iran. Although this move was in support of embargos, it demonstrated how firmware updates could geo-disable module functionality.

Moreover, industrial equipment manufacturers enter into partnerships with cellular module providers. Due to the need for continuous lifecycle management and firmware updates, industrial equipment containing Chinese modules relies on Chinese module manufacturers to maintain and secure their products throughout their serviceable life. This is an undeniable fact.

During a recent UK Government debate regarding the Government Procurement Bill, Chinese modules were brought into the discussion on the grounds of security and market dominance. This was compounded by the discovery of a Chinese tracking device hidden a minister's vehicle in early 2023.

During this debate, Rt Hon Robert Seeley MBE MP was recorded as quoting:

"We know that Chinese Communist party companies such as Huawei actively seek to gain a monopoly position by systematically destroying economic rivals. That is not fair trade; it is trade as a weapon for a Communist party dictatorship. It did it with Huawei, undercutting and deliberately destroying rivals on price through cheap subsidies. It is now doing the same with cellular modules, seeking to dominate and take control of the market. It does that through IP theft, economic espionage, subsidy, access to super-cheap finance, shared technology and other forms of state support.

Companies such as Quectel and Fibocom—the manufacturers of cellular modules—will, like Huawei, claim to be private. They are not."

In conclusion, millions of Chinese cellular modules are integrated into Western industrial equipment, running substantial amounts of Chinese code. While their affordability has made them a popular choice, security concerns exist due to potential vulnerabilities and the **dependence on Chinese manufacturers** for maintenance and updates. These factors highlight the importance of carefully evaluating the risks and benefits associated with using such modules in critical infrastructure.

Western infrastructure faces three significant challenges that can be likened to loaded guns, each with its potential risks:

Security Risk: Cellular modules are essentially communication computers that come with software code provided by the module manufacturer. Due to their communication capabilities, they can establish connections with remote servers. Moreover, all cellular devices can utilize the location of connected cell towers as a reference for tracking purposes. This combination of communication and location features poses potential security risks, as these modules could be exploited for tracking and unauthorized access.

Remote Maintenance: Throughout their active lifespan, cellular modules require regular software and firmware updates. These updates are vital to maintaining security and stability, especially in response to network operator updates. Western nations find themselves heavily reliant on Chinese cellular module manufacturers to ensure the safety and security of critical industrial products throughout their usable life. Without ongoing support from these manufacturers, the modules may become insecure or prone to instability, posing risks to critical infrastructure.

Supply Dependence: A pressing concern lies in the risk of becoming entirely reliant on Chinese module manufacturers to connect critical infrastructure. The perceived government subsidies benefiting Chinese manufacturers may eventually disadvantage Western players, leading to potential crippling effects on their market presence. In this scenario, every nation would be dependent on Chinese suppliers to establish and safeguard their critical infrastructure, raising concerns about sovereignty and independence.

These challenges underscore the importance of a balanced and careful approach in evaluating the risks and benefits associated with using Chinese cellular modules in Western infrastructure. Governments and industries must take **proactive measures** to address security vulnerabilities, ensure continuous support and maintenance, and diversify their supply chain to mitigate potential risks in the long term.

Products, names, logos and designs described herein may in whole or in part be subject to intellectual property rights. The information contained herein is provided “as is.” No warranty of any kind, either expressed or implied, is made in relation to the accuracy, reliability, fitness for a particular purpose or content in this document. This document may be revised at any time.