TLP:WHITE

5G GENERATION

The FBI's Office of Private Sector, in collaboration with the FBI's Intelligence Coordination Working Group, Thomson Reuters Special Services (TRSS), and Deloitte provide this interactive infographic product on the Fifth Generation or 5G technology. This product provides a brief, high-level perspective. The videos and citations reflect the views of the originators.

5G OVERVIEW

According to the **National Institute of Standards and Technology**, 5G wireless communication systems include a wide range of new technologies that can handle more data faster. 5G can transmit voice, data, and images in many ways that need "smart" antennas to connect various types of users at different categories of frequencies/signal strengths. For example, direct cellphone to cellphone connection that can bypass cell towers; and, base or cell towers receiving and transmitting signals can become high-density short communications connection points.

CROSS-SECTOR BENEFITS

The **Institute of Electrical and Electronics Engineers (IEEE)** states, "5G is an enabler of exciting use cases that will transform the way humanity lives, works, and engages with its environment." The IEEE audio/video provides an overview of 5G, its impact across sectors/industries, and the private-public sector collaboration efforts to enhance security and expansions.

According to the **US Federal Communications Commission**, 5G is a technological advancement that can impact economic growth, education, employment, transportation, and more. By year 2020, major global telecommunication operators, internet, and mobile hardware companies are actively developing resources to meet the projected commercial rollout of 5G.

WIRELESS TECHNOLOGY GLOBAL LANDSCAPE

According to Deloitte, the global telecommunications industry leaders in 5G are the United States, Taiwan, Sweden, Finland, China, Japan, and South Korea.

According to the **Intelligence and National Security Alliance (INSA)**, US leadership in 5G technology faces challenges in areas impacting the US economy:

Fewer Wireless Infrastructure Sites - Since 2015, Chinese companies outspent the United States by approximately $24 billion on wireless communication infrastructure, building 350,000 new sites while the United States built fewer than 300,000.

Higher Foreign Research and Development Researchers - Universities in China, Korea, and Taiwan filed more patents than the United States. There are more foreign Information and Communications Technology graduate student researchers in US academia than US students; these students then work for US companies, before returning to their homeland with US technology knowledge.

Foreign Semiconductor Dominance Attempts - Foreign governments, particularly Japan, South Korea, Taiwan, and China, have made attempts to dominate semiconductor technology through government-funded R&D and the use of company acquisition techniques to undermine the US semiconductor industry.

Offshore Manufacturing Costs Benefits - The US telecommunications industry has shifted to off-shore manufacturing, fabrication, and packaging to lower costs and labor.

Image source: Freepik.com

Click for Video: The International Telecommunication Union's (ITU) 5G Overview

Click for Video: The IEEE 5G Overview

Click for Video: The ODNI's Supply Chain Management - Know the Risk, Raise Your Shield

SUPPLY CHAIN DEPENDENCIES

The **Office of the Directorate of National Intelligence's (ODNI)** video on **Supply Chain Risk Management**: ODNI indicated risks and vulnerabilities can be mitigated by knowing vendors and integrating acquisition offices to ensure information security.

According to Deloitte, 5G infrastructure consists of wireless/network service providers, consumer electronics manufacturers, and vendors. TRSS reporting includes semiconductor manufacturers, and satellite service providers to 5G development and deployment. In addition to hardware and service provider dependencies, INSA advises that software and hardware are paramount security concerns as US telecommunication evolves.

US NATIONAL SECURITY IMPLICATION

According to the **ODNI's National Counterintelligence and Security Center**, government-corporate partnerships, and remaining ahead of China are crucial to advancing US 5G security, as well as, global competitiveness:

> Federal government officials warned about the risks and challenges of rolling out 5G wireless networks – particularly in terms of the threat China poses in its global advancement of 5G – and emphasized that use of public-private partnerships in developing America's vision for 5G networks will be critical for ensuring network security and staying internationally competitive.

According to INSA, the use of foreign components, devices, and/or 5G network poses national security concerns, specifically in the counterintelligence arena, as well as, US and allied communications security and reliability during US joint operations. According to TRSS, 5G networks will require constant monitoring given the increase in entry points to the network. The use of foreign technology in the United States 5G core networks can expose US telecommunications and data infrastructure, including those of the US military and intelligence community, to foreign adversaries.

Disclosure is not limited.

TLP:WHITE

I-190815-014

INFORMATION SHARING & ANALYSIS UNIT
FEDERAL BUREAU OF INVESTIGATION
OFFICE OF PRIVATE SECTOR