General Assembly 1

Setting rules and regulations for the jamming of satellites

Research Report

Leiden Model United Nations 2024

"Out of this world"

Forum: General Assembly 1

Issue: Setting rules and regulations for the jamming of satellites

Position: President of the General Assembly

Introduction

Satellites play a critical role in modern communication, navigation, weather monitoring, and military operations. They enable global connectivity, drive economic development, and enhance disaster management. However, as reliance on satellite technology grows, so do the risks to its security. One pressing concern is satellite jamming, a deliberate disruption of satellite signals through radio frequency interference. This issue affects both civilian and military systems, threatening global stability and the functioning of critical infrastructure.

Satellite jamming occurs when a signal is intentionally sent to interfere with the communication link between a satellite and its ground station or users. This disruption can prevent the satellite from transmitting or receiving signals properly. While jamming is non-destructive, its impact can be far-reaching, from interrupting emergency services to compromising national security. The growing availability of jamming technology, coupled with the increasing number of satellites in orbit, makes addressing this challenge more urgent than ever.

Several major actors are involved in the debate surrounding satellite jamming. Countries like the United States, Russia, and China are both developers and targets of satellite jamming technologies, reflecting the geopolitical stakes in space. Private companies such as SpaceX and OneWeb, which operate satellite constellations, are also deeply affected, as jamming can disrupt their services. International organisations like the International Telecommunication Union (ITU) play a key role in managing satellite frequencies and addressing interference issues. However, global efforts to regulate jamming remain limited, as nations prioritise their strategic interests.

The causes of satellite jamming are diverse. Some states use jamming to assert dominance or deny access to communication services during conflicts. Non-state actors, including insurgent groups, may deploy jamming to disrupt military operations. Even unintentional interference, caused by overlapping frequencies or poorly managed systems, contributes to the problem. Technological advancements have made jamming devices cheaper, smaller, and more accessible, increasing the risk from various actors worldwide.

The consequences of satellite jamming can be severe. On the civilian side, it can disrupt vital services such as internet connectivity, GPS navigation, and aviation communication. For militaries, jamming can compromise strategic operations, reduce situational awareness, and put national security at risk. Economically, businesses reliant on satellite services may face financial losses, and consumers may experience reduced access to technology.

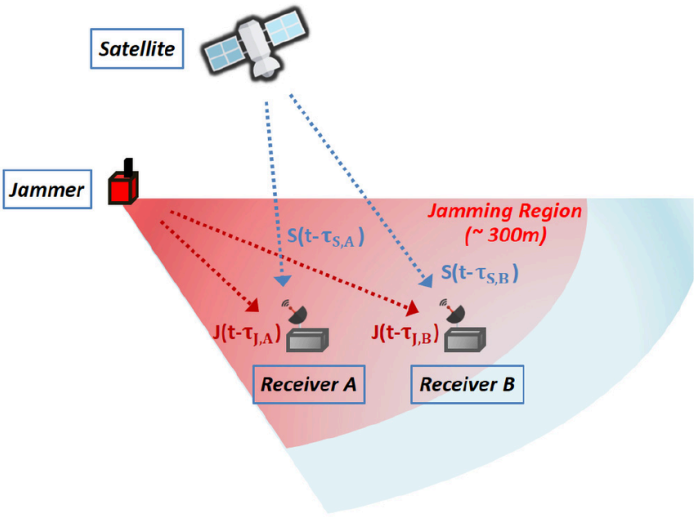
Despite the clear dangers, addressing satellite jamming is complex. Existing international laws are often vague or insufficient, and enforcement is challenging due to difficulties in identifying and attributing jamming activities. Furthermore, the rapid growth of

satellite networks and the increased presence of private actors in space complicate regulatory efforts.

Definition of Key Terms

Satellite jamming

Satellite jamming is an electronic form of warfare where a jammer sends a signal on the same frequency as a satellite's communication signal, thereby preventing it from receiving legitimate transmissions. There are two primary types of satellite jamming: uplink jamming and downlink jamming.



Uplink Jamming

Uplink jamming occurs when interference signals are directed from a ground station or terminal toward a satellite. The interference signal is transmitted at the same frequency as the uplink signal intended for the satellite, which confuses the satellite's receivers. This type of jamming requires more powerful transmitters since the signal must travel vast distances to reach the satellite, but it can disrupt communication across large areas, impacting all users connected to the satellite.

Downlink Jamming

Downlink jamming affects the signals that satellites send back to the ground. In this case, the jammer transmits interference signals at the same frequency as the downlink signal. Downlink jamming usually has a more localised impact because the jammer must be within the line of sight of the receiving terminal, such as a ground station, vehicle, or aircraft. However, its effectiveness is limited to the range of the jammer's coverage area.

Low Earth Orbit (LEO)

Low Earth Orbit (LEO) is the region of space 500 to 2,000 kilometers above the Earth's surface. Satellites in LEO are widely used for communication, Earth observation, and scientific missions. They provide low-latency, high-speed data transmission compared to geostationary satellites. Their closer proximity to Earth makes LEO satellites ideal for internet services like Starlink and precision navigation systems. However, LEO's dense traffic makes it more susceptible to jamming and interference. The rapid growth of LEO constellations is transforming global connectivity while raising concerns about space security.

Frequency Spectrum

The frequency spectrum refers to the range of electromagnetic frequencies used for communication, including satellite data transmission. Specific bands of the spectrum are allocated for different purposes, such as GPS, the internet, and military communications. Managing this spectrum is crucial to avoid interference. Jamming uses this by targeting a specific frequency range to disrupt operations. Global organisations like the International

Telecommunication Union (ITU) regulate spectrum usage. With increasing satellite launches, efficient spectrum allocation is critical to prevent overlapping signals and ensure safe and reliable communication.

Anti-Satellite (ASAT) Weapons

ASAT weapons are systems designed to disable or destroy satellites. They include kinetic tools like missiles and non-kinetic methods like jamming, lasers, or cyberattacks. ASAT capabilities are a strategic advantage in modern rivalry, as they can disrupt an enemy's communication, surveillance, and navigation systems. Major players like the U.S., Russia, China, and India have demonstrated ASAT capabilities. While kinetic ASAT weapons cause debris, jamming is less destructive but equally effective in compromising satellite operations. ASAT weapons raise ethical and legal concerns under international space treaties.

Encryption

Encryption is the process of encoding data to ensure it is accessible only by authorised users. In satellite communications, encryption protects signals from being intercepted or tampered with during transmission. This is a key countermeasure against jamming and hacking attempts. Advanced encryption methods can make jamming less effective by ensuring the satellite distinguishes legitimate signals from interventions. Governments and private companies are investing in quantum encryption to further enhance satellite security. Encryption also plays a role in safeguarding sensitive data from cyberattacks targeting satellites.

Space Sovereignty

Space sovereignty refers to a nation's authority over its space assets, such as satellites. Countries are responsible for protecting these assets from threats like jamming, hacking, or physical attacks. However, space sovereignty raises legal and ethical questions in international conflicts, where satellite jamming might violate another nation’s rights. The concept is governed by international treaties like the Outer Space Treaty, which seeks to ensure peaceful use of space. Balancing sovereignty with global cooperation is a critical issue as space becomes increasingly militarised.

Electronic Warfare

Electronic warfare (EW) involves using electromagnetic signals to disrupt, degrade, or intercept communications and systems. In space, EW includes satellite jamming, spoofing, and cyberattacks targeting satellite networks. EW has become a key aspect of modern conflicts, with countries investing heavily in counter-satellite capabilities. The rise of advanced EW tools threatens not only military operations but also civilian infrastructure like GPS and internet services. Governments and international bodies are working to regulate EW activities to prevent escalations and protect global communication systems.

Major Parties Involved

United States

The United States leads in both satellite deployment and the development of countermeasures against jamming. Organisations like the Space Force and NASA collaborate with private companies to secure satellite communications. The USA. also invests heavily in identifying and mitigating jamming incidents, particularly in areas of geopolitical tension.

China

China is rapidly advancing its satellite programs and has reportedly developed robust ASAT capabilities. It uses satellite jamming as a part of its broader electronic warfare strategy. China's advancements raise concerns among other nations, particularly as it grows its influence in regions like the South China Sea.

Russia

Russia has been accused of using satellite jamming during military operations, particularly in Eastern Europe. It has developed systems designed to disrupt communications, particularly GPS signals, in areas of conflict. These actions have raised alarms about the potential misuse of jamming technologies in warfare.

European Union (EU)

The European Union is a significant player in satellite communication, with programs like Galileo (navigation) and Copernicus (Earth observation). The EU works through agencies like the European Space Agency (ESA) and the European Commission to develop secure satellite systems resistant to jamming. While individual EU countries, such as France and Germany, have their own military space programs, the EU collectively advocates for stricter international regulations on satellite jamming. The EU also emphasises the need for international cooperation to address jamming threats and maintain space security.

India

India is an increasing space power, with growing satellite capabilities in navigation (NavIC), communication, and Earth observation. The Indian Space Research Organisation (ISRO) manages the country’s civilian satellite programs, while its military focuses on developing space defense systems. India demonstrated its ASAT capabilities in 2019 by destroying a satellite in orbit. As a member of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), India advocates for global regulations to prevent weaponization in space, including addressing the threat of jamming.

International Telecommunication Union (ITU)

The ITU is a UN agency responsible for managing the global radio frequency spectrum and orbital slots for satellites. It plays a critical role in preventing satellite jamming by ensuring fair spectrum distribution and addressing frequency interference. The ITU works with national regulators to reduce the risk of intentional jamming and promotes collaboration among member states. However, its authority is limited, as enforcement relies on national governments. The ITU advocates for updated policies to address modern challenges like jamming in an increasingly crowded orbit.

North Korea

North Korea has been accused of using satellite jamming as part of its electronic warfare strategy. It has targeted GPS signals in South Korea and other neighboring regions, often disrupting air and maritime operations. Despite its limited space capabilities, North Korea's use of low-cost jamming equipment highlights the accessibility of this technology. The country's actions raise regional tensions and emphasise the need for international agreements to prevent abuse of jamming technologies by states with limited accountability in global forums.

Private Sector Companies

Private companies like SpaceX, OneWeb, and Amazon are major players in satellite communication, launching large constellations of low Earth orbit (LEO) satellites. These companies are vulnerable to jamming, as they provide services like global internet coverage and precision navigation. Companies invest in encryption and

anti-jamming technologies to protect their networks. However, the private sector also pressures governments to develop international regulations to ensure the security of commercial satellites. Their growing influence makes them critical contenders in debates over space security and jamming prevention.

United Nations Office for Outer Space Affairs (UNOOSA)

UNOOSA manages international cooperation in the peaceful use of outer space. It facilitates dialogue among nations to address challenges like satellite jamming, advocating for space sustainability and security. UNOOSA is a key player in shaping policies that align with the Outer Space Treaty, which forbids the militarisation of space. While it lacks enforcement power, UNOOSA plays a vital role in promoting transparency and encouraging international collaboration to address the risks posed by jamming technologies.

Middle Eastern Countries

Countries in the Middle East, such as Iran and Saudi Arabia, are increasingly involved in satellite technology and its potential misuse. Iran, for example, has been accused of jamming international satellite broadcasts to control information within its borders. Meanwhile, Saudi Arabia invests heavily in satellite infrastructure for communication and surveillance. The region's geopolitical tensions often lead to the use of jamming as a tool for electronic warfare or political control. These activities highlight the need for regional and international efforts to address jamming threats.

General Overview

Causes of Satellite Jamming

Military and Strategic Objectives

Satellite jamming is often used as a military tactic to gain a strategic advantage. Militaries use jamming to disrupt enemy communication, navigation, and surveillance systems. By targeting GPS signals, for example, an attacker can reduce the precision of guided missiles, disorient forces, or create confusion during operations. Jamming offers a low-cost, non-destructive means to weaken an opponent's capabilities without escalating to direct confrontation. Unlike kinetic attacks, such as destroying a satellite, jamming is reversible. Once the jamming device is turned off, normal functionality can be restored.

Countries like Russia, China, and the United States are heavily involved in developing advanced jamming capabilities. For instance, Russia's Krasukha-4 system can jam satellite-based radar systems over large areas. These military tools are often tested during exercises or regional conflicts, raising concerns about the increasing sophistication and accessibility of jamming technology.

Geopolitical Disputes

Satellite jamming is also used as a tool of political leverage or censorship. Governments may block communication satellites to suppress dissent, limit the spread of information, or demonstrate their technological prowess. For example, during political unrest, governments in regions like the Middle East have been accused of jamming international broadcasting satellites to block news coverage critical of their regimes. This reflects broader conflicts over information control and freedom of speech.

Countries involved in territorial disputes may use jamming as a way to assert dominance or disrupt activities they view as encroaching on their sovereignty. For instance, during tensions in the South China Sea, reports of GPS jamming affecting ships and aircraft raised alarms about the use of electronic warfare in contested regions.

Cybersecurity Concerns and Espionage

Satellite systems are increasingly targeted in cyberattacks aimed at disrupting services or stealing data. Jamming is often used as a first step in these operations, making satellites vulnerable to following attacks. For example, state-sponsored hackers might use jamming to disable a satellite's communication links, making it easier to break its security protocols.

Non-state actors, such as terrorist groups and independent hackers, also use jamming for harmful purposes. For example, disrupting navigation systems can create chaos in critical sectors like transportation or energy. Cyber-jamming, which combines traditional jamming techniques with advanced hacking, poses a growing threat to satellite infrastructure.

Commercial Competition and Industrial Sabotage

The commercial satellite industry is highly competitive, with companies competing for control over profitable markets such as telecommunications, broadcasting, and satellite internet. While rare, instances of industrial sabotage through jamming have been reported.

For example, one company might jam a competitor's satellite signal to disrupt its services, causing customer dissatisfaction and financial losses. Although illegal and unethical, such actions highlight the intense competition in the satellite market.

As the demand for satellite-based services grows, companies are under pressure to protect their systems from both deliberate and accidental interference. This has led to increased investment in anti-jamming technologies and improved safety measurements.

Accidental Interference

Not all jamming is intentional. Accidental interference occurs when equipment emits signals on frequencies used by satellites. This can happen due to poorly maintained devices, such as malfunctioning radios or wireless networks. Accidental jamming is more common in regions with weak technology regulations or outdated equipment.

For example, during large events, the use of unregulated communication devices can overwhelm satellite systems, causing unintended disruptions. In 2015, U.S. military officials reported an average of 23 cases per month of accidental satellite interference, highlighting the seriousness of this issue.

Consequences of Satellite jamming

Disruption of Communication Services

One of the most immediate effects of satellite jamming is the disruption of communication services. Satellites provide vital links for mobile networks, television broadcasts, and internet connections. Jamming can interrupt these services, affecting millions of users. For example, during political protests, governments in some countries have used jamming to block communication satellites, preventing people from organising or sharing information.

The disruption of communication services can also have severe economic consequences. Businesses that rely on satellite connectivity for operations, such as banks, logistics companies, and broadcasters, face significant losses when services are interrupted. The impact is particularly severe in remote areas where satellite communication is the primary means of connectivity.

Threats to Navigation and Transportation

Satellite navigation systems, such as GPS, are critical for transportation, aviation, and maritime operations. Jamming GPS signals can cause ships and planes to lose their way, leading to delays, accidents, or even collisions. For example, during conflicts in Eastern Europe, reports of GPS jamming affecting civilian flights raised concerns about the safety of international air travel.

Jamming also affects ground transportation systems that rely on GPS for navigation and tracking. This includes emergency vehicles, which may be delayed in reaching their destinations, and logistics companies, which face disruptions in supply chain operations.

Economic Losses

The economic impact of satellite jamming is significant. Disrupted services can lead to downtime, lost revenue, and increased operational costs for businesses. For example, telecommunications companies may need to compensate customers for interrupted services, while satellite operators may incur costs for moving satellites to avoid interference.

The cost of repairing or replacing damaged equipment also adds to the financial burden. For instance, satellites affected by prolonged jamming may need to adjust their orbits, consuming valuable fuel and reducing their lifespan. These costs are ultimately passed on to consumers, increasing the price of satellite-based services.

National Security Risks

Satellites play a critical role in national security, providing communication, surveillance, and navigation capabilities for military and intelligence operations. Jamming these systems can weaken a country's ability to respond to threats or coordinate defense efforts. For example, during conflicts, jamming military satellites can prevent troops from receiving critical instructions or accessing real-time intelligence.

Jamming also poses risks to homeland security by disrupting systems used for disaster response, border control, and infrastructure monitoring. For instance, emergency services that rely on satellite communication may face delays in coordinating relief efforts during natural disasters.

Environmental and Safety Concerns

Prolonged jamming incidents can contribute to environmental and safety risks. For example, satellites affected by jamming may need to adjust their orbits, increasing the risk of collisions with other objects in space. This can create additional space debris, further complicating satellite operations.

On the ground, disruptions to navigation systems can lead to accidents in critical sectors such as aviation and shipping. These incidents highlight the broader implications of jamming on public safety and environmental sustainability.

Loss of Trust in Satellite-Based Technologies

Frequent jamming incidents can damage public trust in satellite-based technologies. If users cannot rely on GPS for navigation or satellite internet for communication, they may be less willing to adopt these technologies. This could slow down innovation in emerging sectors such as autonomous vehicles, remote healthcare, and smart cities.

For businesses and governments, the loss of trust in satellite systems can have long-term consequences. Companies may face challenges in attracting customers or securing investments, while governments may struggle to implement policies that depend on satellite infrastructure.

Timeline of Events

1960s **Early Development of Satellite Communication**

The first communication satellites were launched, allowing for global communication. Early satellite jamming efforts were primarily military, intended to disrupt enemy communications during the Cold War.

1970s **Development of Jamming Technology**

Jamming technology began to be refined, particularly for military applications. Countries like the U.S. and the Soviet Union developed techniques to jam satellites, especially during conflicts and military operations.

1980s **First Incidents of Satellite Jamming**

Satellite jamming began to be used in various international conflicts, particularly in the Middle East, where nations attempted to disrupt communications using jamming devices targeting satellite links.

1990s **Commercial Satellite Growth**

The rise of commercial satellite services, such as television broadcasting and communications, expanded the vulnerability of satellites to jamming. This period saw increased awareness of the importance of satellite security.

2001 **U.S. Military Jamming Incidents**

Following the September 11 attacks, the U.S. military faced several jamming incidents, which caused disruptions in satellite communications, highlighting the need for better defense mechanisms against jamming attacks.

2007 **China's Anti-Satellite Test**

China conducted a successful anti-satellite (ASAT) missile test, destroying one of its own weather satellites. This test raised concerns over the militarisation of space and the potential for satellite jamming and other anti-satellite activities.

2011 **Increased Satellite Jamming in the Middle East**

Satellite jamming incidents were reported in the Middle East, particularly in countries like Iran, where the government used jamming to block satellite television and internet signals. This was one of the first large-scale, non-military uses of jamming to control information.

2014 **Global Satellite Jamming Incidents**

Several countries reported disruptions to satellite communications. These included both accidental and intentional jamming, which highlighted the growing risks posed by jamming to both civilian and military satellites.

2016 **United Nations Discusses Space Security**

The UN Office for Outer Space Affairs held discussions on space security, focusing on satellite interference, including jamming. This marked a growing international recognition of the need for cooperation and regulation regarding satellite security.

2018 **U.S. Warns of Russian Satellite Jamming**

The U.S. Department of Defense issued a warning regarding Russian efforts to disrupt communications from satellites, particularly those used by the U.S. military. This brought global attention to the use of satellite jamming in geopolitics.

2020 **Commercial Satellite Operators Targeted**

Satellite constellations operated by companies like SpaceX and OneWeb began to experience jamming incidents, which disrupted internet services in regions such as the Middle East and Africa, indicating that private satellite networks were increasingly at risk.

2023 **International Efforts to Address Satellite Jamming**

The International Telecommunication Union (ITU) and other international bodies began working on stronger regulations to prevent satellite jamming and coordinate efforts to secure satellite communications, signaling an increased focus on the security of space infrastructure.

Possible Solutions

Strengthening International Rules and Cooperation

One solution to satellite jamming is to create stronger international rules and improve cooperation among nations. Organisations like the International Telecommunication Union (ITU) could lead efforts to make clear laws about the use of satellite frequencies and the banning of jamming activities during peacetime. Countries could also agree to a treaty that defines punishments for those who intentionally jam satellites. By working together, nations can improve how they detect and trace jamming incidents, making it harder for attackers to act without being identified. Clear and shared rules would reduce conflicts and build trust between nations, protecting satellite operations globally.

Developing Advanced Anti-Jamming Technologies

Investing in advanced technology is a key step in stopping satellite jamming. New tools, like anti-jamming antennas and encrypted signals, can make it harder for attackers to interfere with satellites. Technologies such as frequency-hopping and beamforming can reduce the risk by making satellite signals harder to target. Artificial intelligence could help

by detecting and blocking jamming attempts in real time. These technologies make jamming more expensive and less effective for attackers. Governments and private companies should work together to fund research and bring these innovations to life, ensuring satellites stay secure and reliable even under threats.

Encouraging Public-Private Partnerships

Public-private partnerships (PPPs) can bring together the strengths of governments and businesses to tackle satellite jamming. By working together, they can share information about jamming incidents and create better strategies for dealing with threats. These partnerships can also focus on building more secure satellite systems, such as constellations with backup satellites to keep communication running smoothly. Governments could provide funding to private companies and startups to develop affordable and innovative anti-jamming solutions. Training programs and joint exercises would prepare both sides for real-world challenges, creating a united and effective response to satellite jamming threats.

Bibliography

'10 Things: What's That Space Rock? - NASA Science'. Accessed 2 November 2024. https://science.nasa.gov/solar-system/10-things-whats-that-space-rock.

'Baylon-Ccyberspace-En-1-1129.Pdf'. Accessed 2 November 2024. https://swfound.org/media/205523/baylon-ccyberspace-en-1-1129.pdf.

'Catalog of Earth Satellite Orbits'. Accessed 29 September 2024. https://earthobservatory.nasa.gov/features/OrbitsCatalog.

Flores, Maya E., Devon D. Poisson, Colin J. Stevens, Adriyel V. Nieves, and Alexander M. Wyglinski. 'Implementation and Evaluation of a Smart Uplink Jamming Attack in a Public 5G Network'. *IEEE Access* 11 (2023): 75993–7. https://doi.org/10.1109/ACCESS.2023.3296701.

'IADC'. Accessed 29 September 2024. https://www.iadc-home.org/documents_public/view/search_field/eNortjI2tlJy1CsuTcpKTS7RdtTLS8xNBVIlielAMjk_ryQ1r6RYyRpcMAypDUU~/page/1/id/126#u.

'Impact of Rocket Launch and Space Debris Air Pollutant Emissions on Stratospheric Ozone and Global Climate - PMC'. Accessed 28 October 2024. https://pmc.ncbi.nlm.nih.gov/articles/PMC9287058/.

'Impacts of Large Satellite Constellations on Astronomy: Live Updates | American Astronomical Society'. Accessed 29 September 2024. https://aas.org/posts/advocacy/2021/08/impacts-large-satellite-constellations-astronomy-live-updates.

'India's First "military" Satellite GSAT-7 Put into Earth's Orbit'. Accessed 28 October 2024. https://www.ndtv.com/india-news/indias-first-military-satellite-gsat-7-put-into-earths-orbit-533526.

'Intergovernmental Oceanographic Commission of UNESCO (IOC-UNESCO) | International Coral Reef Initiative'. Accessed 28 September 2024. https://web.archive.org/web/20170725143015/http://www.icriforum.org/about-icri/members-networks/intergovernmental-oceanographic-commission-unesco-ioc-unesco.

ITU. 'Regulation of Satellite Systems'. Accessed 28 October 2024. https://www.itu.int:443/en/mediacentre/backgrounders/Pages/Regulation-of-Satellite-Systems.aspx.

'Low Earth Orbit Definition & Meaning - Merriam-Webster'. Accessed 2 November 2024. https://www.merriam-webster.com/dictionary/low%20earth%20orbit.

'Material Selection for a CubeSat Structural Bus Complying with Debris Mitigation - ScienceDirect'. Accessed 2 November 2024. https://www.sciencedirect.com/science/article/abs/pii/S0273117720308383.

‘Regulating the Next Generation of Satellites | BCG’. Accessed 2 November 2024. https://www.bcg.com/publications/2024/regulating-the-next-generation-of-satellites.

‘Satellite Jamming | On the Radar’. Accessed 28 September 2024. https://ontheradar.csis.org/issue-briefs/satellite-jamming/.

‘Uplink Jamming, Technique EX-0016.01 | SPARTA’. Accessed 20 October 2024. https://sparta.aerospace.org/technique/EX-0016/01/.

‘WRS-24 – ITU World Radiocommunication Seminar 2024 (WRS-24)’. Accessed 29 September 2024. https://www.itu.int/wrs-24/.