The dual role of satellite internet in fragile contexts: opportunities for development and challenges for security

by Gaetano Sicolo

Today's global society has become increasingly reliant on digital infrastructure and connectivity. The growth of technology and the ability to stay connected offer an opportunity for low- and middle-income countries (LMICs) to close the digital gap and accelerate their development. One key aspect of this change is the rapid rise of satellite Internet, which offers fast and affordable connectivity in unserved and underserved communities.[1]

"The growth of technology and the ability to stay connected offer an opportunity for low- and middle-income countries (LMICs) to close the digital gap and accelerate their development

While it may sound like science fiction, this same technology has been exploited by terrorist and violent extremist groups operating in fragile regions to facilitate their operations. It has been demonstrated that such groups use satellite-based communications to coordinate operations in remote areas and spread propaganda in places that were previously inaccessible.[2]

The role of satellite networks in developing contexts

Digital technologies and Internet connectivity can drive development, especially in LMICs, as being connected provides better access to information and increases communication, along with new opportunities for learning and work. While this appears positive, the impact of these benefits depends on factors such as infrastructure availability, service affordability, access to devices, connection security, and the population's level of digital literacy skills.[3]

These positive factors led the United Nations to prioritize universal connectivity as a goal to achieve by 2030,[4] with satellite connectivity having the potential to increase both fixed and mobile broadband access in areas where fiber Internet is scarce. Economically, studies show that a 10%

1 International Telecommunication Union, "Managing Spectrum for Evolving Technologies", *ITU News Magazine*, No. 5, 2019.
2 Global Initiative Against Transnational Organized Crime, "Risk Bulletin of Illicit Economies in West Africa", Issue 12, May 2025.
3 International Telecommunication Union, "Achieving Universal and Meaningful Digital Connectivity: Setting a Baseline and Targets for 2030", 2021.
4 United Nations, "Roadmap for Digital Cooperation", Report of the Secretary-General, 2020.

rise in Internet penetration can boost gross domestic product (GDP) per capita growth by 2% to 2.3% for fixed broadband and 2.5% to 2.8% for mobile broadband in developing countries.[5]

Economic growth, in turn, leads to improvements in education and healthcare. Higher-quality education boosts literacy rates and, consequently, digital literacy, addressing one of the main barriers to Internet use along with affordability.[6] At the same time, satellite Internet has been used for telemedicine and remote diagnostics in rural areas that lack resident doctors or sufficient medical infrastructure, providing a solution for countries where building terrestrial infrastructure is challenging.[7]

> **"In the Sahel and wider Sub-Saharan Africa, criminals not only exploit Starlink terminals but also smuggle them across the region into countries where it is still illegal**

Although satellite connectivity has the potential to provide both universal and meaningful coverage, the same features that make satellite networks advantageous also introduce vulnerabilities.

In fragile regions, terrorist and violent extremist groups can exploit these technologies to coordinate operations and spread propaganda, illustrating the double-edged nature of this emerging technological infrastructure.[8]

Security risks and misuse by violent extremist organizations

When considering the nexus between transnational organized crime and terrorism, new technologies should be

5 International Telecommunication Union, "Economic Impact of Broadband in LDCs, LLDCs and SIDS: An Empirical Study", 2019.

6 International Telecommunication Union, "ICTs, LDCs and the SDGs: Achieving Universal and Affordable Internet in the Least Developed Countries", 2018.

7 Eutelsat, "Telehealth for Remote Communities".

8 Gaetano Sicolo, "Dark Signals: The Growing Threat of Satellite Internet in Extremist Networks", *Global Network on Extremism & Technology,* 2024.

viewed within a broader context. Terrorists and violent extremists have been increasingly using digital platforms for two main reasons: to promote extremist content and to coordinate agendas.[9]

In the past, groups like the Islamic State West Africa Province (ISWAP) relied on slow, high-latency satellite Internet to communicate with other extremist organizations in the region.[10] For their needs, Thuraya Wi-Fi offered Internet access at 60 Kbps within a 30-metre range, but that changed with the arrival of Starlink. Starlink uses Low-Earth Orbit (LEO) satellites, allowing higher download speeds of around 200 Mbps in areas lacking stable terrestrial networks.[11]

In the Sahel and wider Sub-Saharan Africa, criminals not only exploit Starlink terminals but also smuggle them across the region into countries where it is still illegal.[12] Unfortunately, this offers numerous advantages to these threat actors, enabling them to gain an edge over national forces and use instant messaging applications to spread propaganda or recruit new fighters.

Looking ahead, satellites may become increasingly targeted by cyber-attacks by violent extremists as their technological capabilities advanc- Currently, satellites perform essential military functions, and many global services rely heavily on this infrastructure. This dual-use nature indicates that a successful attack could have far-reaching consequences beyond vulnerable regions. It also underscores the importance of viewing space-based communication networks as critical infrastructure, since their disruption could have widespread impacts.[13]

Satellite networks as critical infrastructure

Identifying infrastructure as critical allows governments to recognize and address its vulnerabilities, and satellite networks are among the most exposed to malicious interfer-

9 Folahanmi Aina et al., "The "Webification" of Jihadism: Trends in the Use of Online Platforms, Before and After Attacks by Violent Extremists in Nigeria", *Global Network on Extremism & Technology*, 2023.

10 Malik Samuel, "ISWAP's Use of Tech Could Prolong Lake Chad Basin Violence", *Institute for Security Studies,* 2023.

11 Abdoulaye Mamane, 'Signature d'accord sur l'internet haut débit: Global licensing and activation I Starlink s'engage à fournir l'internet haut débit au Niger', *Le Sahel,* 2024.

12 Global Initiative Against Transnational Organized Crime, "The Shadow Constellation: How Starlink Devices Are Shaping Conflict and Crime in the Sahel", *Observatory of Illicit Economies in West Africa,* Issue 12, 2025.

13 Meghan Bartels, "Why Satellites Need Cybersecurity Just Like You", *Space.com,* 2018.

ence. Radiofrequency attacks such as spoofing are already widespread and require limited technical expertise.[14] Recent civil aviation data illustrate the scale of the threat: on average, 1,500 flights per day were affected by spoofing in 2024, with more than 41,000 incidents recorded between July and August alone.[15]

Satellites and the broader space ecosystem should be regarded as critical infrastructure, precisely because they support national security, public health, economic activity, and the functioning of modern societies. In practice, they are connected to nearly every vital sector, and studies have indicated that a successful cyber-attack could disrupt these sectors within just 12 hours.[16] This risk was highlighted during the U.S. *Hack-A-Sat* competition, where ethical hackers demonstrated how vulnerabilities in satellite systems could be exploited if not properly secured, emphasising the urgency of adopting stronger security standards to prevent malicious actors from exploiting the same weaknesses.[17]

"Identifying infrastructure as critical allows governments to recognize and address its vulnerabilities, and satellite networks are among the most exposed to malicious interference

The current approach to satellite security remains fragmented. Some national strategies classify space assets as part of critical infrastructure, but international coordination remains limited.[18] New constellations are being launched faster than security frameworks can adapt, resulting in significantly higher costs for responding to major incidents, especially in sectors that rely heavily on satellite networks.

As satellite constellations continue to grow and more services move to space-based networks, the question is no longer whether they should be protected but how. This urgency calls for coordinated strategies to safeguard satellites while enabling their development potential. The next step is to consider what those strategies might look like.

Conclusion and recommendations

The momentum generated by satellite infrastructure needs careful management, considering both its growth potential and risks. As mentioned earlier, its disruption could trigger a chain reaction across critical sectors, from communications and transportation to public health and emergency services. Given the importance of these systems, governments cannot protect them alone; instead, a collaborative approach involving international organizations, private operators, and Member States would be more effective.

While coordination mechanisms already exist under the International Telecommunication Union and the Committee on the Peaceful Uses of Outer Space (COPUOS), they should be strengthened and better aligned, moving from voluntary reporting[19] to mandatory public-private threat responses. Ensuring the proper

14 Nicolò Boschetti et al., "Commercial Space Risk Framework Assessing the Satellite Ground Station Security Landscape for NATO in the Arctic and High North", *IEEE*, 2022.

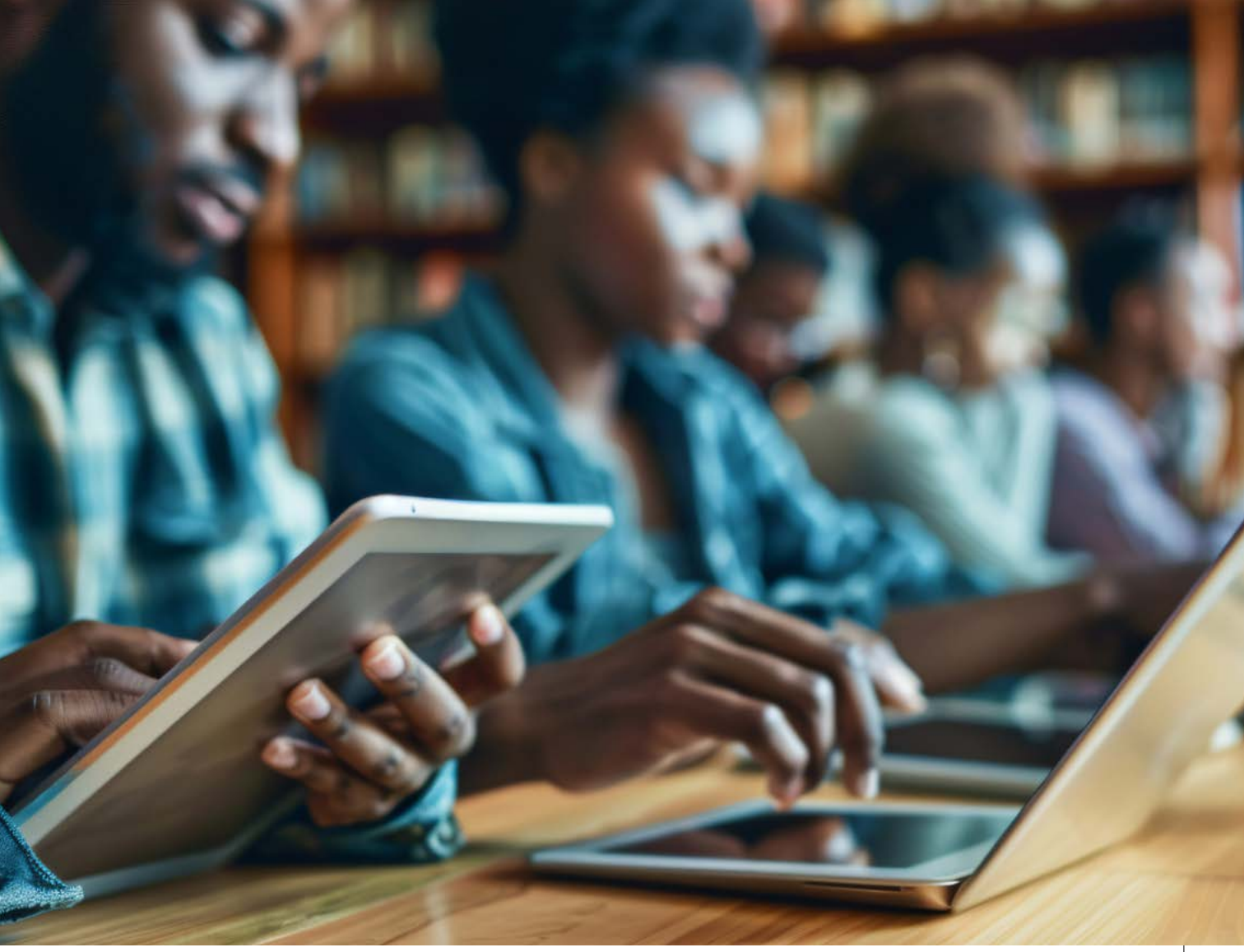
15 Ops Group, "Final Report of the GPS Spoofing workgroup", 2024.

16 Linda Dawson, "Life Without Satellites in War in Space", *Springer*, 2018.

17 Brett Tingley, "These 3 Teams Just Hacked a US Air Force Satellite in Space... and Won Big Cash Prizes", *Space.com*, 2023.

18 Rian Davis et al., "Space as Critical Infrastructure: An In-Depth Analysis of U.S. and EU Approaches", *Acta Astronautica*, vol. 225, 2024.

19 United Nations Office for Outer Space Affairs, "Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space", 2021.



operation of satellite networks should be a top priority, and security strategies should focus on making sure that the benefits are not compromised by their vulnerabilities. As developing regions expand their Internet access, much of their growth will depend on the safety and affordability of space-based communication systems. Therefore, strengthening cooperation among Member States, international organizations, and private companies will be crucial to bridging digital gaps and ensuring that satellites are consistently protected as critical infrastructure.

> **“As satellite constellations continue to grow and more services move to space-based networks, the question is no longer whether they should be protected but how**

ABOUT THE AUTHOR

Gaetano Sicolo is a graduate student in Area and Global Studies for International Cooperation at the University of Turin, with research experience in geopolitics, technology, and security. He has contributed to the work of the Global Network on Extremism and Technology and the Institute for the Analysis of International Relations (Istituto Analisi Relazioni Inter nazionali), producing analyses on the implications of digital connectivity, satellite internet, and violent extremism in Sub-Saharan Africa.