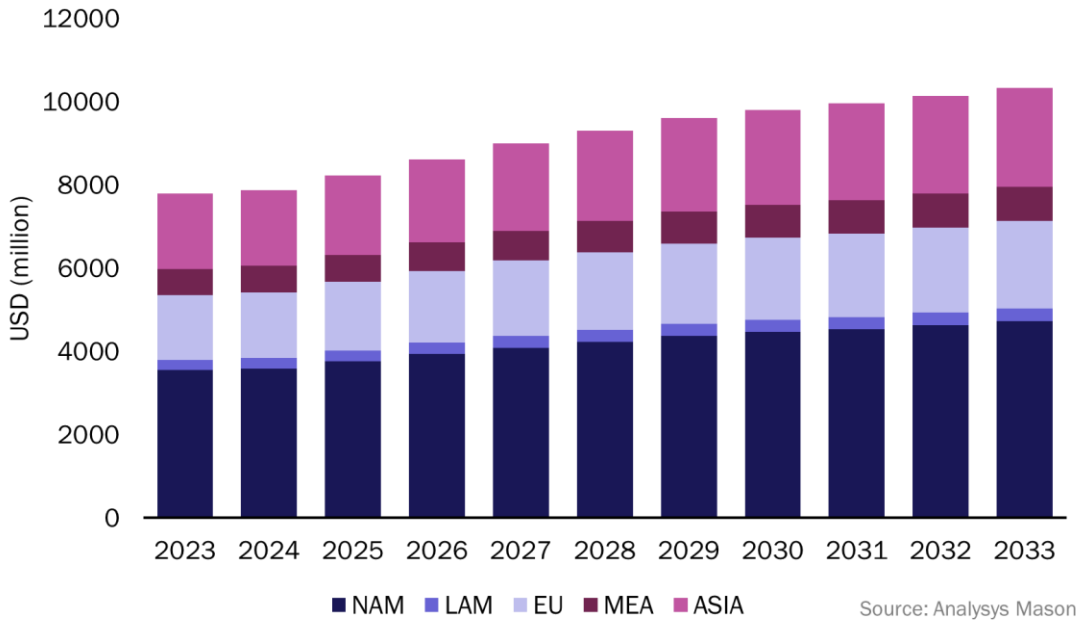
Commercial PNT actors can address public GNSS spoofing and jamming risks to generate new revenue

October 2024

Sarah Halpin

Players in the commercial satellite market have an opportunity to address government and wider industry concerns about the reliability, resiliency and security of traditional positioning, navigation and timing (PNT) services (including historically free services such as GPS) by developing new revenue-generating services. PNT services play an essential role in supporting many critical functions across society, from tracking uber driver locations to enabling military UAV long-distance missions. Indeed, Analysys Mason's report *The positioning, navigation and timing (PNT) market: a framework for understanding the satellite industry revenue opportunity* discusses how commercial PNT players have an opportunity to capitalise over the next 10 years on a **USD10.3 billion revenue opportunity** in the defence market.

Figure 1: Forecast revenue for the defence market, worldwide



PNT services play an essential role in helping to protect against threats to Global Navigation Satellite System (GNSS) services. GNSS refers to satellites that broadcast their locations in space and time, with networks of ground control stations and receivers that calculate ground positions by trilateration (that is, using distances to determine location).

A loss of PNT services (for example, due to technical failures or malicious activity) could have potentially disastrous consequences, both in terms of safety risks (such as preventing aircraft locations from being tracked) and economic risks (for example, a British government report found that a 24-hour GNSS outage alone could result in a USD1.82 billion loss to the economy). Security-associated issues have been an area of focus for the

industry during recent discussions of GNSS services because of the increasing levels of spoofing and jamming attacks worldwide.[1]

New government GNSS solutions can reduce spoofing and jamming risks, but threats remain; this is a clear market opportunity for commercial players

Spoofing refers to the purposeful manipulation of GNSS signals to fool the end user into believing that the signal is originating from a false location. Jamming refers to the purposeful overpowering of a signal to prevent PNT data from being sent. For example, the maritime and aeronautical industries have reported concerns about growing levels of jamming near areas of conflict such as Ukraine. Geopolitical instability is also leading to increasing debate about the accessibility and security of PNT services that originate from countries of concern (such as Russia and its GLONASS GNSS service). Such essential services could be suddenly switched off as a result of these shifts in geopolitical standing. Governments are also examining potential risks to national security via external PNT services.

With governments now actively assessing these risks to PNT service security, we are seeing increased develop new dedicated PNT services in systems, for example, for use in some countries in Africa and South Korea, as well as upgrades to legacy systems, including new GPS satellites. Governments are also investigating the use of new receiver technology. For example, the US government has stated that it plans to purchase m-receivers, which allow focused power to (theoretically) overcome a jamming signal. Such technology will reduce, but not eliminate, such risks.

Commercial players should consider their ability to address the spoofing and jamming challenges as an enabler of revenue opportunity

New technologies take time and money to develop and there are challenges to be overcome with government legacy systems. However, commercial players such as satellite operators and satellite service providers are in a position to manufacture and launch services quickly to address these challenges. They can capture new revenue either directly (by developing their own services), or indirectly (via partnerships with PNT companies to offer PNT as a service).

For example, interoperability and layering of assets is a growing approach to satellite security, which means that there is space for government and commercial activity in tandem. This is further supported by the overall benefits of engaging with commercial services, allowing customers to cut development costs and increase the speed at which new services are delivered.

Resilience in these service types is a requirement, and commercial entities are actively developing a responsive PNT services market. The commercial PNT industry is nascent, but interest is growing in commercial PNT assured services (that is, technologies that aim to prevent natural and human-caused disruptions to GNSS) and alternative services (for example, technologies that ensure that PNT services are reactivated should they become

[1] For more information, see SpaceNews (28 August 2024), *US leaders have been warned to focus on GPS and PNT to protect the nation* and Breaking Defense (9 October 2024), *To attack enemy space capabilities, Army eyes doubling expert cadre*.

unavailable). These quickly evolving developments in the PNT market mean that there is strong revenue potential available for assured and alternative players.