Preparing for a Loss of Position and Timing

Summary of a roundtable held on Thursday 30th November 2023

This was a hybrid event held in person at Pool Re, London and online via MS Teams. The meeting was held under the Chatham House Rule.

Meeting Chair: Lord Toby Harris – Chair, National Preparedness Commission

Report Authors: John Pottle - Director, Safety Navigation, Royal Institute of Navigation
Andy Proctor - Chair, PNT Advisory Group, Royal Institute of Navigation

The roundtable was convened to discuss the important issues raised in a paper prepared for the NPC by the Royal Institute of Navigation, Preparing for a Loss of Position and Timing. The Chair set the scene by drawing participants' attention to the ubiquity of reliance on satellite-derived positioning, and the vulnerability of these systems to multiple threats, including space weather and geomagnetic activity (the Met Office now publishes a daily forecast from its Space Weather Operations Centre to help system owners to predict adverse events – a step in the right direction).

Report co-author, John Pottle began the discussion by outlining some of the key points made in the report:

- Since the report was published, government has announced a PNT Framework. This is an appropriate approach which enables a systems engineering approach to PNT resilience, and formation of the Framework is a seminal point. Threat actors jamming or 'spoofing' systems are increasing, not least in connection with geopolitical tensions, which heightens the level of risk to PNT integrity.
- The Framework contains a 10 Point Plan which includes an update to the current alerting protocols to include mitigation measures. Government has also created a PNT Office, which works across government, and is a welcome development.
- The report describes an 'uncomfortable over-reliance' on satellite-derived position and time. This reliance is largely a result of its low cost combined with a high degree of accuracy, with the discomfort coming from awareness of the vulnerability of satellites to multiple threats, some of which cannot be predicted with any degree of confidence.
- A scenario in the paper illustrated the speed with which communications, supply chain and other services, including financial trading, would grind to a halt following any significant disruption.
- PNT is perhaps better described as 'TPx' – timing, which gives position, which in turn enables a host of other functions, including navigation.

Reflecting on this exposition of the problem, participants made several observations:

Firstly, stakeholders in sectors reliant on distribution technology - such as retail or logistics - may not have understood the need to test business recovery plans to work without the benefit of PNT, believing the system to be far more resilient that it is. In fact, the National Risk Register suggests that the severity of impact of a PNT loss event may range between moderate and catastrophic, and the likelihood may be as high as 1 in 20 over a 2-year timescale. Casual jamming incidents are reported to happen up to 200 times a day. Clearly, then, it behoves such operators to investigate their own risk exposure and ensure plans are in place to mitigate that risk. Some tools to help with this are available on the RIN website, bearing in mind that the steps to take will vary depending on the circumstances of the event.

Secondly, investment is needed to address the issue at a strategic level, mitigating risks from various perspectives and putting in place contingency measures. The technology itself may be vulnerable to cyber-attacks, for example. In the area of timing, global supply chains will be significantly impacted by GNSS failure, requiring complicated recovery and contingency plans. This raises the important question of global PNT assurance and space security – in a connected world it cannot be solely a sovereign matter. GNSS is globally owned and managed, unlike some other satellite arrays.

Thirdly, social systems vulnerability is often overlooked in discussions like these. Cyber can be the trigger for thinking differently about this – cyber and PNT systems are increasingly synonymous. Threats come from bad actors as well as bad weather or space accidents. The services affected will include social services, such as food and healthcare systems. Local Resilience Forums and other social infrastructures are important here, and these are not well enough integrated into the UK Government Resilience Framework.

Fourthly, there is a general lack of understanding of PNT as a utility that is inherently vulnerable. This is not on the planning radar of local authorities, for example, with relation to the impact of their services.

Fifthly, the PNT Office is facing enormous levels of expectation, and it is worth reflecting on the significant achievement represented by publishing the PNT Framework built upon cross-government alignment. The Framework enables financial commitment through Government spending rounds and a mechanism for setting out a PNT resilience agenda in the short-, medium- and longer term. Timing is of particularly critical importance to critical national infrastructures, as well as in Defence – a point which emerged clearly during the development of the Framework.

Andy Proctor, the report's co-author steered the discussion towards potential mitigating actions, starting with the need to continue raising awareness across society using language that anyone can understand, and which helps generate a proper appreciation of the risk. In addition:

- The PNT Office could usefully bring insights together into a useable and accessible framework. This might explain, for example, what happens to assets, including critical assets, in the event of a loss of PNT. What difference does it make to everyday operational contexts?
- Only by understanding assets and their use cases can system owners decide what complementary technology is needed to increase resilience in their particular use case (alongside GNSS which will usually remain primary). These technologies will also have some levels of vulnerability to risk (especially cyber), so will need to be similarly assessed).

- PNT challenges tend to be put into the 'too difficult' box, but now that we have leadership and acknowledgement of the issue from Government, progress is possible. The next step is to bring the elements of the PNT Framework together (eliminating silos), followed by agreement of milestones and targets for improvement.

Discussion continued, including recommendations and exploration of the following themes:

There is a general lack of understanding of systems that are used every day, and how vulnerable they are to jammers – simple gadgets that are illegal to use, yet not illegal to buy or own, and readily available. The ability to govern and prepare society better to deal with this and other threats to PNT is arguably an international concern (as is the case with mobile technology). Removing governance from the government of the day is the first step towards enabling real progress. Best practice guidelines for critical national infrastructure are being developed through the RIN, as well as some investigation as to the extent of existing knowledge and preparedness in each infrastructure. This includes the hidden or unknown vulnerabilities – for example, systems that do not recover after an antenna is unplugged temporarily.

International collaboration has a vital part to play in addressing the problem, however Galileo is the only internationally-governed GPS system (BeiDou in China and Glonass in Russia, being examples of state-governed defence systems, despite being part of the international network). The PNT Office will have to work with others around the world to overcome the siloed thinking. US GPS Advisory Group has a similar role in adapting its requirements to the changing threat landscape, over which it has no direct control. What is needed is not plans, but an adaptable planning infrastructure.

International leadership has been demonstrated by the PNT Office by using resilience as a 'hook' to pull the Framework together and shape engagement with international partners. Further progress might be achieved by emulating the civil aviation approach to incident reporting. Under MOR and VOR (Mandatory/Voluntary Occurrence Reporting) systems, which are adhered to in the interests of safety. Introducing a voluntary version of this for PNT would build datasets that could be collated, anonymised and analysed for the purpose of providing scale and impact assessment data throughout the value chain. This might be an initiative in which RIN could take the lead. It was suggested that some kind of enabling structures would be required to encourage participation – for example to avoid the risk of legal liability that might otherwise deter reporting.

The cyber community has already navigated similar challenges to PNT and there is likely to be much that can be learnt from that experience. The relationship between the two sectors is increasingly interrelated, so closer working is sensible.

Vulnerabilities cannot be seen as a one-off problem with a 'point' solution, but a continuous situation that will evolve as technology and behaviours evolve. This underlines the requirement for an adaptive approach and governance infrastructure, and not simply a strategy. There is a clear opportunity for government to lead, and for industry to follow. However, there is currently not a clear pipeline of knowledge, skills and talent. Skills development must be part of the ongoing PNT programme which transcends government terms of office – UK Skynet is an example of this approach working well in the space industry. The PNT Framework needs to work with the UK Government Resilience Framework in order for this to work well. Civil society plays a major role in both frameworks and could be more overtly written in.

Finally, there was some discussion around the different types of resilience that relate to PNT: technical resilience of the systems; resilience in terms of contingency measures (eg, maps); and resilience of each sector that is reliant to some extent on PNT, for example by including PNT in business continuity plans. Procurement frameworks, for example, need to include SLAs with CNI providers that make reference to PNT loss, thereby making someone responsible for the risk.

It might also be possible to encourage some industries to increase resilience by design, so preventing loss from happening, and there is an opportunity to clarify the roles that various bodies can play. Local authorities, for example, are unlikely to have deep understanding of PNT-related risks, how they might differ from cyber risk, and what might be required to mitigate those risks. It was noted that some recent announcements of major resilience investment do not currently include PNT resilience.

In closing the meeting the Chair thanked participants and suggested that follow-up actions might be coordinated through the RIN. These could include more awareness raising, approaches that are systemic, not bounded by organisational interests, and collaboration on best practice working with a much broader community.