A novel comprehensive risk-based approach for the assessment of the dependency of road transport on GNSS

PhD Candidate
Ashley Brooks[1]

Supervisor
Prof. Washington Ochieng[1]

[1]*Centre for Transport Studies, Department of Civil and Environmental Engineering, Imperial College London*

Abstract

Introduction/background

It has been known since the early development of GPS that while GPS can support economic and civil activity it can also create a dependency. This has given a dilemma for decision-makers who must maximise benefits while minimising risks. Given the capabilities of GPS, rapid growth was clear from the outset and the diversity of applications is impressive. It was also predicted that GPS applications would become deeply embedded in economic activities and increasingly embedded in national and international infrastructure, leading to an increase in potential vulnerabilities.

There is a growing dependence on GNSS. Many systems and devices rely heavily on GNSS-derived data to provide critical services – and this is particularly apparent in cities. These services are wide-ranging and include, for example, location-based services, 3G/4G mobile networks, aviation, emergency services, logistics and (road/rail) transportation, building and construction, banks and financial institutions (timestamping). The European GNSS Agency estimates that 5.8 billion GNSS devices were in use in 2017, forecast to rise to 8 billion by 2020.

However, low power, freely available (and often unencrypted) signals are relatively easy to disrupt and manipulate, whether intentionally or unintentionally. There are many threats to GNSS-dependent systems, leading to inaccurate positioning, navigation and timing (PNT) information or, indeed, none at all. Typical threats include spoofing, interference, GNSS segment errors (upload data, satellite faults), multipath, cyber attacks and atmospheric interference.

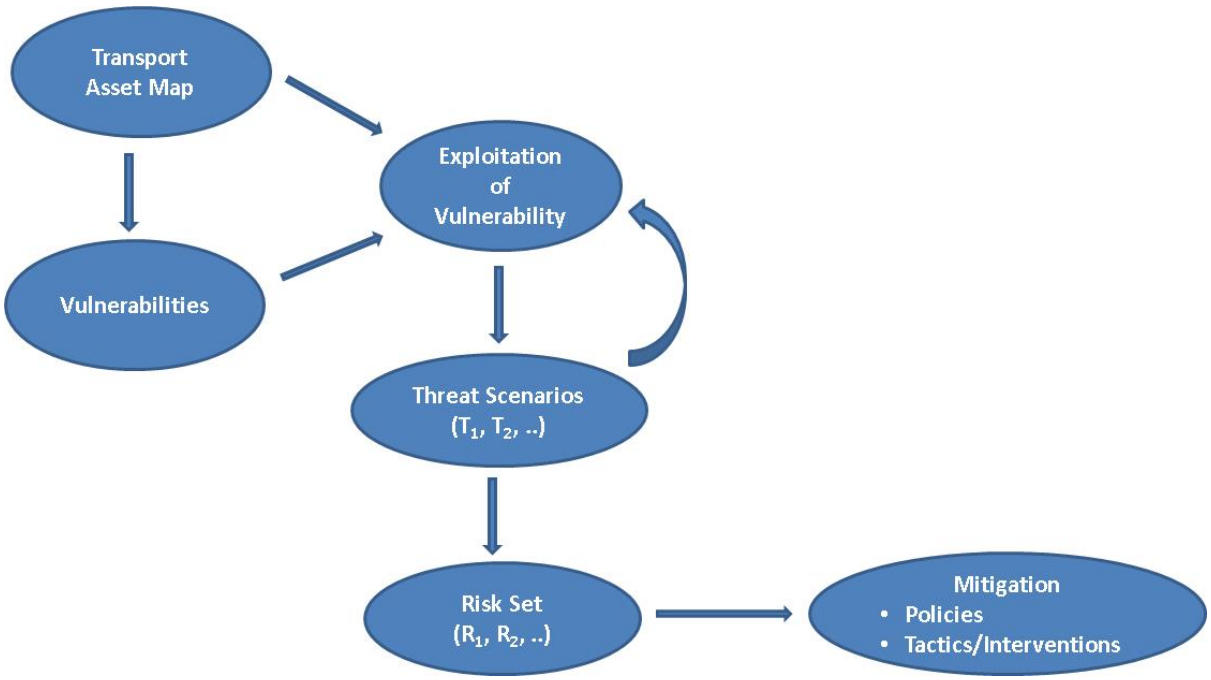
Understanding these threats is vital to perform a reliable risk assessment; this includes understanding the source of the threats, typical location/geography of the threats and impact on the user. At present, this is poorly understood, particularly with respect to system users and designers, and system interdependencies.

This research examines the threats and risks of GNSS for PNT with respect to the UK's Critical National Infrastructure (CNI), officially defined by the UK government – with a particular focus on the Road Transport sector, identified as a key sector with significant utility benefits (~£2 billion) from GNSS (London Economics Report, 2017). Furthermore, the GSA GNSS Market Report 2017 forecasts that the road sector will account for 38% of the GNSS market over the next 5 years. Any disruption of GNSS could severely hit road transport infrastructure and services.

The US Volpe report (2016) provides an inventory of GPS dependencies in the transport sector along with best practices to improve resilience and robustness. However, it does not consider sources of disruption nor potential threats or risks associated with each category of disruption. The report recognises that other critical infrastructure depends on GPS signals, and identifies a number of examples that illustrate the cascading impact on transport if GPS was lost; for example, communications are incorporated into transport systems and there would be a cascading impact on safety-critical functions. However, no detailed analysis on the dependency of road transport on GNSS, and interdependencies between other critical infrastructure, (along with threats and risks) has been carried out.

Methodology

The approach taken to understanding the current and future risks within road transport will be based on the framework, *below*, starting with a detailed specification of the transport asset map (architecture, system boundaries). Once the map has been defined, vulnerabilities can be identified; this will be followed by the various ways of exploiting a vulnerability, leading on to a set of threat scenarios. This will then be turned into a set of risks from which appropriate mitigations may be formulated.

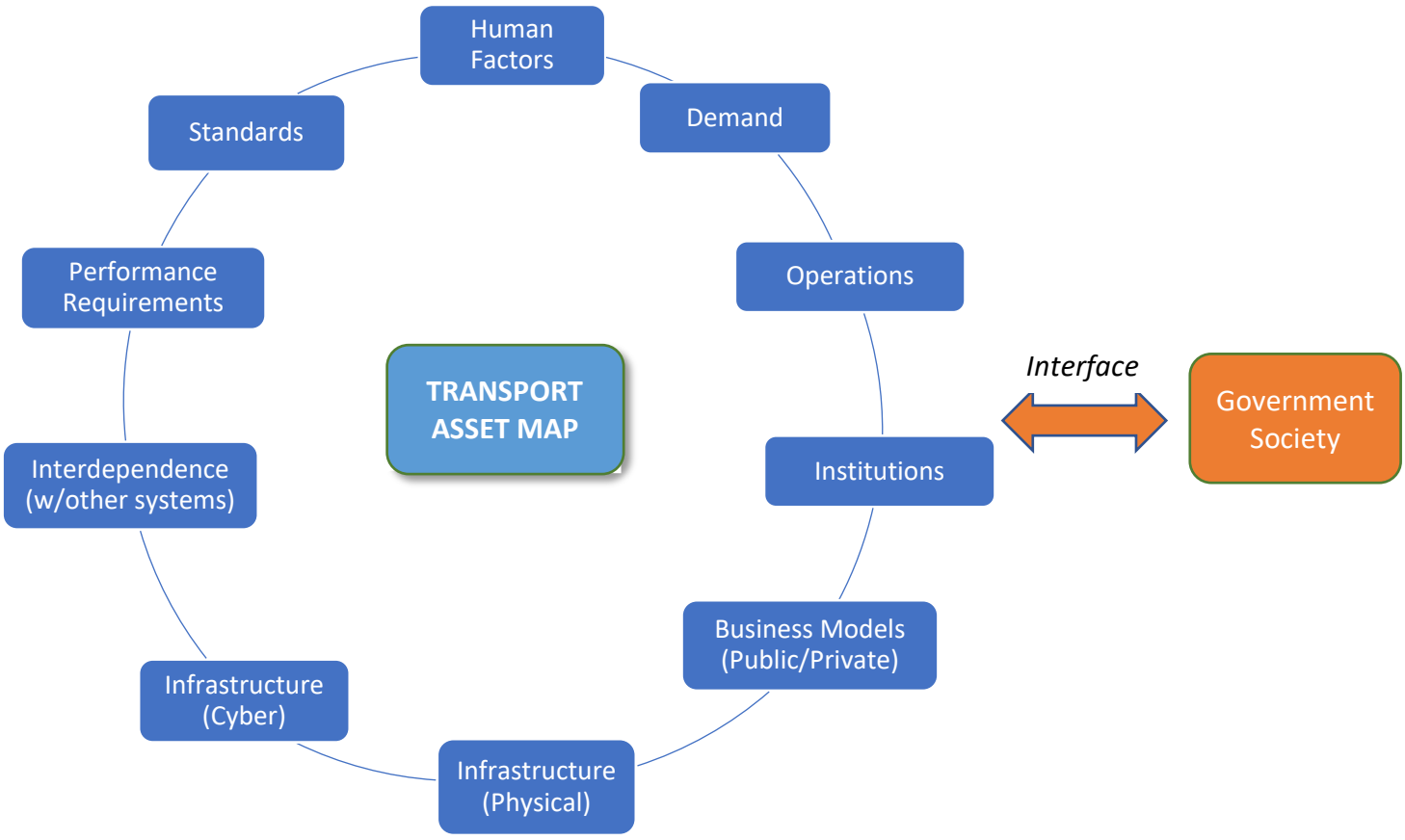


Transport Asset Map (Road sector)

A preliminary Transport Asset Map (TAM) is illustrated, *below*. The TAM is intended to be comprehensive to capture vulnerabilities within the road sector in a comprehensive way. TAM components include*:*

Human factors; Demand; Operations; Institutions; Business models (public/private); Infrastructure (physical); Infrastructure (cyber); Interdependence with other infrastructure/systems; Requirements; Standards.

The TAM sits at the interface with *Government* and *Society*, where the bi-directional arrows indicate that one is influenced/affected by the other, and vice versa.



It is anticipated that within the *Threat Scenarios*, threat vectors such as the following will be identified. However, a comprehensive list will follow on from the *Vulnerabilities*. Some *Threat Scenarios* may emerge from multiple threat vectors.

Anticipated Threat Vectors (not limited to)

Natural/Accidental
1. Built structure obstruction
2. Terrain obstruction
3. Foliage (pines, heavy canopy)
4. Solar Activity – mild
5. Solar Activity - moderate
6. Solar Activity -powerful
7. Human Error/software
8. Satellite malfunction
9. Control Segment Failure
10. Space Debris
11. Unintentional RF

Malicious Acts
12. Privacy seeker (1 event)
13. Criminal Jamming (1 event)
14. Criminal + Privacy (1 year total)
15. Criminal Spoofing (1 event)
16. Terrorist Jamming
17. Terrorist Spoofing
18. Military-style Jamming
19. Nat. Agent Spoofing
20. Attack on Satellites
21. Attack on Control Segment
22. Cyber Attack on Control Segment

Once the *Threat Scenarios* and corresponding *Risk Set* have been detailed a suitable method for risk analysis will be chosen; it is expected that a hybrid method for risk analysis will be taken such as FRAM / SPTA / STAMP, appropriate to a complex system.

Threat Scenarios
Risk Set
} Hybrid method chosen for risk analysis (FRAM / SPTA / STAMP) - suitable for (complex) system

Conclusions/Outcomes

Mitigation

Only then, can appropriate risk mitigation be implemented (with respect to GNSS or alternative PNT systems). This includes carefully chosen, appropriate Policies and Tactics/Interventions along with careful prioritisation. This project seeks to inform UK's CNI policy from a GNSS standpoint and provide a comprehensive risk assessment and mitigation strategy within the road transport sector. However, the approach can be easily extended to other sectors and other nations' infrastructure.