**Implementing Cyber Security Controls in Road-Based Intelligent Transportation Systems (ITS) in London, UK: A Review (<2200 words)**

***Introduction (<220 words)***

**Introduction**

*Context*

Autonomous vehicles and intelligent transport concepts are becoming popular due to their many benefits, including efficiency and cost reduction. By far the most prominent topic being researched regarding transport systems is ITS as part of the smart city concept. The most pressing use for ITS appears to be road networks due to issues, such as congestion.

ITS purposes:

* Reduced fuel consumption
* Reduced CO2 emissions
* Road usage efficiency
* Reduced congestion
* Reduced travel time
* Safer road networks/public safety

ITS Technologies:

* VANET, including V2X communications
  + With UAVs
* CAV

ITS Security:

* Underlying IoT technology often vulnerable.
* Impact of cyber security incident in ITS could harm trust in the road network. User trust is key.

*Aim & Purpose, including justification for review*

Aim: To explore the use of cyber security controls in road network Intelligent Transportation Systems based on London, UK. Exploratory study.

Purpose: ITS systems already being tested in London and will need to be resilient against attack due to the dependency many have on the road network as CNI. This is a proactive identification of key cyber security controls, gaps and opportunities that should be considered to manage the risk to ITS.

***Main Body (<1760)***

**Review Methodology (<220 words)**

*Research Questions*

1. What cyber security tools and techniques have been applied to or recommended for road-based ITS?
2. Which road-based ITS use cases are most applicable to London, UK?
3. What requirements should be considered when designing cyber security controls for ITS? E.g. scalability, 24/7 operation, automation, performance impacts, compatibility with future technologies, etc.
4. How would a threat actor exploit a road-based ITS system and why? (Scope: Intentional attacks – as defined in 2)
5. When will the security of road-based ITS become pertinent to London? How can society prepare for this?

*Approach*

* 1. Broad topic research to create good foundation for literature review, including identifying a suitable timeframe, key words to search, and sources to use based on recommendations of reliable academic digital libraries.
  2. Recorded and categorised relevant references, looking for more recent citations and linked articles.
  3. Defined subtopic of interest (ITS) and chose research questions.
  4. Defined a literature criteria based on research questions.
  5. Look for additional relevant articles based on more specific key words from subtopic
  6. Filter all literature down based on criteria and record the rationale for any omissions.
  7. Use the resulting literature to begin planning and writing the literature review.
  + Sankey diagram showing literature filtering

*Paper Structure*

* Sections
* Conceptual order

**Findings (<770 words)**

*London Use Cases*

* Transport Strategy: [2018](https://tfl.gov.uk/corporate/about-tfl/the-mayors-transport-strategy), “prepare for new technology”
* Surface Intelligent Transport System (TfL): [Background](https://ted.europa.eu/udl?uri=TED:NOTICE:573371-2018:TEXT:EN:HTML&src=0) / [Progress](https://its-uk.org.uk/tfl-and-siemens-deliver-uk-first-next-generation-traffic-signal-technology-in-london/)
* CAV (TfL): [Background](https://tfl.gov.uk/corporate/publications-and-reports/connected-and-autonomous-vehicles)
* Smart motorways (DfT): [Background](https://www.roads.org.uk/articles/smart-motorways) / [Issues](https://www.gov.uk/government/news/smart-motorway-rollout-to-be-paused-as-government-responds-to-transport-committee-report) (shows that a thorough risk assessment should be completed before undertaking work on ITS)

*Threats, Vulnerabilities, Attacks, Cyber Risks*

* Motivations
  + Hacktivism based on recent road protests in London/Ottawa
  + Nation states targeting CNI to disrupt or even cause harm with cyber-physical systems
  + OCG – Data theft, location tracking, etc.
* ITS Attack Vectors
* Smart vehicle specific Attack Vectors

*Cyber Security Tools & Techniques*

Split by [NIST categories](https://www.nist.gov/cyberframework/online-learning/five-functions) – Identify, Protect, Detect, Respond, Recover (Graph)

Controls discussed in the literature – frequency graph (picked top mentioned)

* Encryption
* Authentication
* Blockchain
* Standards, Governance & Regulations
* IDS
* Privacy models
* Security by design

**Discussion (<770 words)**

*Key Themes*

* + Control requirements for ITS, e.g. scalability, device computational power, 24/7 support, real-time data, etc.
  + Challenges of implementing cyber security controls, e.g. large amounts of data, large attack surface, IoT device constraints, etc.
  + Highly automated IoT systems, like ITS, are being met with automated cyber security solutions, e.g. artificial intelligence used for IDS.

*Strengths*

* Security research attempting to keep pace with technology innovations and even pre-empt challenges, e.g. 6G & quantum computing
* Significant recent research available on ITS with a strong focus on resilience and privacy which have emerged as key cyber security issues in recent years.

*Limitations*

* ITS is in its infancy so a lot of the research is theoretical. Either simulation/small-scale testing only. Could be due to lack of data available, including lack of up to date, realistic datasets for security testing.
* Straightforward use cases only. Consider edge cases and emergencies with regards to security
* More focus on scalability and latency of security solutions, such as authentication, than on security/resilience to attack.
* Not holistic solutions, e.g. one uses HTTP for testing.

*Gaps*

* Lack of agreed and enforced standards/guidelines for security (secure by design)
* Incident Response: How would stakeholders manage roles, responsibilities and operations in the event of an ITS cyber incident?

***Conclusion (<220 words)***

**Conclusion**

*Answers to Research Questions, if possible*

Technological development is increasing in pace year on year so it is inevitable that these challenges will surface in the near future. ITS is being tested on a small-scale in London but proactive consideration for security is required to ensure the implementation does not succumb to the same pitfalls as other IoT.

*Future Research*

* Testing theories on larger datasets or even real-world ITS would strengthen knowledge in the field.
* The lack of standardisation in IoT could have a knock on impact on ITS and there is lots that could be learnt from existing research into wider IoT applications, such as industrial applications.
* Industry View: What are the security perceptions and views of those building the smart city/ITS projects?

**Limitations**

* Thorough but not exhaustive search that will have been influenced by choice of key words and digital libraries. Also the search was limited to freely accessible sources in the English language.
* Some information on emerging technologies, such as ITS, is closely guarded due to their commercial value.

**References**

[Export from Mendeley]