Australasian Transport Research Forum 2021 Proceedings
8-10 December, Brisbane, Australia
Publication website: http://www.atrf.info

Dynamic assessment of regulation and policy framework in the cybersecurity of Connected and Autonomous Vehicles

Shah Khalid Khan, Nirajan Shiwakoti, Peter Stasinopoulos

School of Engineering, RMIT University

Melbourne, Australia

Email for correspondence: s3680269@student.rmit.edu.au; shahkhalid_k@yahoo.com

Abstract

CAVs (Connected and Autonomous Vehicles) technology will transform the current Intelligent Transportation System (ITS). However, the most significant challenge is keeping up the criminal justice system, particularly the Regulation and Policy Framework (R&PF) in ITS, because ubiquitous CAVs connectivity expands the scope of criminal activity in both the physical and cyberspace realms. This article developed a Causal Loop Diagram-based System Dynamic model that incorporates critical inter-disciplinary parameters and dynamically evaluates the impact of R&PF on CAVs cybersecurity. Two loops are envisioned: "balancing loops" demonstrate how R&PF can facilitate cyber-attacks prevention, whereas "reinforcing loops" reveal how imposing R&FP can negate its potential benefits by creating a detrimental parallel circle. Based on the feedback loops, a "shifting the burden" system archetype is postulated in which governments combat cyber-threats by strengthening R&PF while also reducing CAVs adaptation through imitation and induction. Recommendations for R&PF formulation include a balanced approach to the trade-off between: i) protection of CAV users' privacy and freedom, ii) operational and data accessibility constraints on CAV automakers and service providers, as well as their business investment protection, and iii) state regulators command and control thresholds.

1. Introduction

The introduction of CAVs (Connected and Autonomous Vehicles) will fundamentally alter the existing transportation landscape. CAVs at Levels 4 and 5 can detect their surroundings and navigate autonomously by using: i) a variety of sensors (camera, radar, lidar), ii) 3D holographic display, and iii) vast amounts of data analysed in the Intelligent Transportation System (ITS) (SAE-International, 2018). The evolution of this transition necessitates that the CAV be administered as a cyber-physical system-a collaborative network of electronic components that regulate mechanical elements. This has prompted new partnerships between technology companies and traditional automakers, broadening the scope of criminal activity in both the physical and cyberspace (Khan et al., 2020e).

The CAVs deployment is expected to result in various economic benefits, including more equitable transportation, improved public health and social welfare (Haratsis et al., 2018), reduced environmental degradation, and increased road safety . Despite these advantages, a significant source of concern for CAVs stakeholders (technology companies, financial institutions, users and automakers) is a lack of clarity in Regulation and Policy Frameworks (R&PF)-which could impede the widespread CAVs roll-out (Khan et al., 2021a). The present legal framework is seen as a barrier to the potential community advantages of CAVs in terms

of safety, productivity, environmental, and mobility improvements (Dosen et al., 2017, Khan et al., 2021a). The primary source of this anxiety is the ramification caused by the ubiquitous CAV connectivity within the ITS, which has resulted in a slew of regulatory caveats across multiple jurisdictions. These avenues are: i) data confidentiality, privacy concerns, and operational safety during CAVs operation in ITS, ii) short-term economic considerations, public infrastructure, as well as social and economic issues surrounding private car ownership, ridesharing, and employment, and iii) insurance liability in the event of an accident.

Moreover, in the event of a successful cyber-attack, these concerns would be heightened, i.e., determining the liability and accountability of perpetrators in the dynamically integrated CAV-based ITS operation is highly challenging. Cyber-attackers have been dubbed "modern-day pirates," and cyber-insurance has been proposed. It is, however, a two-edged sword: it is both a part of the problem and a solution. It would ease the cost of corporate investment while also providing a veneer of legitimacy for ransom payments.

R&PF are critical components of CAVs cybersecurity. While CAVs Levels 3-5 are still being tested, regulatory authorities should develop standards for CAV deployment and take the necessary steps to ensure the cyber-safe operation of CAVs in ITS (Noy et al., 2018). However, the regulation is challenging when the commercialization of the end-user's data results in profit for some parties at the expense of the end-user. Additionally, the integration of technology and automakers necessitates a dynamic and interconnected analysis of CAVs R&PF. Nonetheless, the criminal justice system is struggling to keep up with technological advancements in transportation.

1.1 The rationale of the study

Academics and industry are equally interested in the R&PF that governs the functioning of CAVs in ITS. Numerous researchers have assessed and emphasised the importance of regulations governing CAVs cybersecurity in various aspects (Cabinet Office, 2016, Hodge et al., 2019). Nevertheless, current research lacks a system-wide foresight analysis that employs the System Dynamics (SD) approach to dynamically assess the R&PF governing CAVs cybersecurity in ITS (Sterman, 2000, Khan et al., 2021a, Khan et al., 2021b).

There is "nested complexity" when a sophisticated organisational (ITS) and policymaking structure (regulators) governs a physical system (CAV). Understanding "nested complexity" is an important first step towards properly integrating the three components (technology, organisations, and policy) for a cyber-safe CAV-based ITS. It will highlight the critical role of R&PF in CAVs cybersecurity and its implications on CAVs adoption. To the best of knowledge, the scope of R&PF in CAVs cybersecurity has not yet been synthesised in a fundamental system-oriented approach. CAVs in the ITS are highly complex and dynamic, involving many stakeholders and a large number of interactions between them.

1.2 Causal Loop Diagram

The Causal Loop Diagram (CLD) based SD approach-a subset of system theory seeks to synthesise and comprehend complex systems' behaviour. CLDs are analysed in terms of behaviour patterns, with more intuition and more profound knowledge (Forrester, 1958, Sterman, 2000). Because CAV technology is constantly evolving, and there is a scarcity of empirical data on the use of R&PF in CAV cybersecurity. Therefore, CLD is a suitable research technique for developing a unified suite of high-leverage technologies and policies for CAVs cybersecurity.

There has been little research on SD in CAVs, but it does examine CAVs deployments and acceptance. The SD approach is used by Stanford (2015) to assess the effect of CAVs adoption on ITS. Using the SD method, Nieuwenhuijsen et al. (2018) investigated the long-term proliferation of CAVs. In addition, Stasinopoulos et al. (2020) investigated the impact of CAVs adoption on the use-stage life cycle gas emissions using the SD approach. Nevertheless, (Khan et al., 2021a) intrducted a conceptual diagrahm for cybersecurity assessment of CAVs based on CLD, as well as stock and flow model for CAV cybersecurity (Khan et al., 2021b).

1.3 Contribution of the study

We conducted an integrated dynamic evaluation of the impact of R&PF on the cybersecurity of CAVs. The key contributions are listed below:

- We developed a CLD-based SD model that incorporates key inter-disciplinary factors pertinent to the R&PF in CAVs cybersecurity.
- Based on the CLD, we identified two types of feedback loops: i) "balancing loops," which show how R&PF may aid in cyber-attack prevention, and ii) "reinforcing loops," which demonstrate how enforcing R&FP can negate its potential advantages by generating a destructive parallel cycle.
- Balancing loops and reinforcing loops triggered a system archetype-"shifting the burden". The system archetype illuminates the underlying structures, providing natural leverage for successful system modifications.
- Additionally, we proposed recommendations for developing an appropriate R&PF for CAVs cybersecurity.

The remainder of the paper is structured as follows. The next section outlines the methodology adopted. Section 3 elaborates the conceptual CLD-based SD Model. The following section describes the feedback loops and system archetype. Section 5 focuses on discussion and policy recommendations. The limitations and future extensions of the study are finally presented in Section 6.

2. Methodology

To investigate the complex, interconnected, and uncertain impact of R&PF on CAVs cybersecurity, we used a CLD-based SD approach, a technique that has the potential to investigate the system-level cybersecurity implications of self-driving cars (Sterman, 2000, Stasinopoulos et al., 2020, Khan et al., 2021b, Khan et al., 2021a). CLD visualises model composition using intuitive graphical diagrams, determines key factors, generates feedback loops, and identifies a system archetype. The use of system archetypes enables the efficient improvement of systems. System archetypes may be used as a diagnostic tool to identify behavioural patterns that have developed an undesirable situation. CLD is used to assess the security of SAE 4 (or higher) self-driving vehicles through the lens of a functional pathway (SAE-International, 2018).

3. Proposed structure of the Causal Loop Diagram

The model variables and their mapping are based on solid innovation theory, i.e., meta-exploratory quantitative analysis of post-2010 literature derived from various sources, including peer-reviewed journal databases, books, and doctoral dissertations, and credible company surveys; augmented with forward/backward snowballing. This leads to identifying critical avenues that are crucial to assess the impact of R&PF on CAVs cyber-safety research.

The following section discusses each parameter's scope, significance, and influence in the model and provides references.

Additional aspects such as CAVs communication technology, human considerations, trust, and hacker capability are outside the scope of this study. This choice is mainly motivated by the need for a restricted border when assessing limited parameters, as well as the non-geographical character of the SD model, although these features are essential for future research.

3.1 The Causal Loop Diagram (CLD) development

The CLD consists of nodes and edges. Nodes represent the variables, and edges represent the relationships between the variables. In a positive causal relationship, both nodes increase in the same direction. In contrast, in a negative relationship, as one node grows, the other decreases, thus implying that the two variables move in opposite directions. The two closed cycles, reinforcing and balancing, are essential features of CLDs. Reinforcing loop: change in one direction is compounded by additional change, and balancing loop: change in one direction is countered by a change in the opposite direction. The arrow with two small lines indicates the presence of a delay sign.

The proposed architecture of the CLD for R&PF in the CAVs cybersecurity is depicted in Fig.1. The scope of various variables included in CLD (Fig.1) is summarised in a consolidated tabular description, along with references in Table 1. The linking of independent and dependent variables in terms of cause and effect, potential impact as a process, polarity (positive or negative influence), and uncertainty is shown in Table 1. Because there is a dearth of empirical evidence, the uncertainty rating in Table 1 is based on our study of available literature and logical conjecture.

Table 1: Factors influencing Regulation and Policy Framework (R&PF) in the CLD.

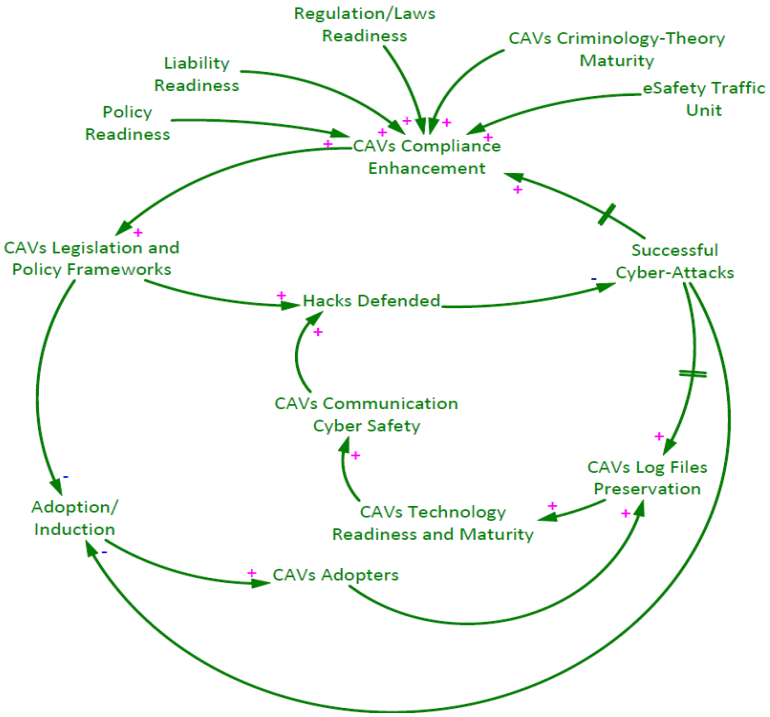
Independent Variable	Dependent Variable	Impact as Process	Uncertainty	Polarity	Sources
Policy Readiness	Compliance enhancement	The essence of the policy decisions taken, both nationally and globally, on how CAVs will be accommodated and what type of vehicle autonomy will be enabled is the most significant impact on the need (or lack of need) for infrastructure transformation in ITS. Policies are typically the driving force behind the legislation. Clear and concise policies for CAVs operation will facilitate cyber-safe CAV-supported ITS.	High	+	(Geels and Penna, 2015, Taeihagh and Lim, 2019, Johnson, 2017).
Regulation/Laws Readiness	Compliance enhancement	Given the ubiquitous nature of cyber-attacks, hacktivists tend to seek out and exploit legal loopholes. The operating guidelines should cover insurance procedures, crash guidelines, acceptable autonomous vehicle ethical conduct, data storage and tracking of communication data, e.g., Licensing and permits-issuing of a CAV user license after CAV safety education.	High	+	(Seuwou et al., 2020, Hodge et al., 2019, Liu et al., 2020).

Liability Readiness	Compliance enhancement	A supporting factor for enhancing compliance is defining a clear liability.For example, in the event of a damage-causing incident (such as the Tesla accident), the liability that regulates the law must be clearly defined. The liability requirements are likely to be settled incrementally on distinctly restricted grounds through legal precedent on navigation and crash avoidance systems in the near term.	High	+	(Rosique et al., 2019, Lederman et al., 2016)
CAVs Criminology-Theory Maturity	Compliance enhancement	Criminal design is often an afterthought in developing new technology and is rarely considered from the start of innovation of new technology, as is the case with CAVs technology. The pervasiveness of CAV connectivity broadens the scope of crimes committed in both cyberspace and physical space in ITS. The criminological theory aids in comprehending CAVs cyber-crimes and criminal justice, thereby improving CAVs compliance enhancement.	High	+	(Newton, 2017, Elzen et al., 2004).
eSafety Traffic Unit	Compliance enhancement	The nature of CAV operation in ITS necessitates the use of L&PF at all levels, from state to national to worldwide. Therefore, new authority, i.e. the esafety Traffic Unit, with pre-existing expertise and new dynamic CAVs operating knowledge, will make it easier to combat cyber-physical space crimes. Similarly, gaining a better understanding of the motivations of CAVs hackers may contribute to the creation of hacker countermeasures	Medium	+	(Uzair, 2021)
Compliance enhancement	Regulation and Policy Framework (R&PF)	Robust CAVs regulatory laws and policy framework are driven by integrating policy readiness, regulation/laws readiness, liability readiness, CAVs Criminology-Theory Maturity, and eSafety Traffic Unit	High	+	(Khan et al., 2020e, Feng et al., 2020).
Regulation and Policy Framework (R&PF)	Hacks defended	R&PF would have established policies and strategies that would aid in the prevention of cyber-attacks.	High	+	(Seuwou et al., 2020, Liu et al., 2020, Khan et al., 2021a).
Hacks defended	Successful Cyber-Attacks	The high number of hacks being defended will minimise the number of successful CAVs cyber-attacks.	High	-	

Regulation and Policy Framework (R&PF)	Adoption and Induction	The regulatory and policy framework of CAVs would impact a variety of dimensions, such as privacy, confidentiality, operational safety, short-term economic considerations, public acceptance, ethical and legal issues. Governments counter the perceived cybersecurity threat of hackers (high successful attacks) by enhancing the regulatory laws and policy framework. Users then perceive that action as creating barriers to their freedom. So, users respond by decreasing imitation, which slows CAVs adoption and induction.	Medium	-	(Seuwou et al., 2020, He, 2018, Khan et al., 2021a).
Adoption (From Imitation and Innovation)	CAVs Adopters	In terms of adaptation, the Bass Diffusion Model (BDM) adequately explains CAVs penetration, i.e., adoption by imitation and adoption by innovation. Two essential parameters of BDM are: i) the product's attractiveness and ii) effectiveness of persuading potential adopters, known as the coefficient of innovation.	Medium	+	(Bass, 1969, Sterman, 2000).
Induction (From Imitation and Innovation)	CAVs Adopters	Induction includes public transit users, cyclists, children and some elderly because of the availability of CAV. The induced demand tends to be a typical reaction to decongestion in car-centric environments by public transit users.	Medium	+	(Mewton, 2005, Williams et al., 2020)
Successful cyber-attacks	Adoption and Induction	Successful cyber-attacks will impact the product's attractiveness and effectiveness of persuading potential adopters, known as the coefficient of innovation.	High	-	(Sterman, 2000).
Successful cyber-attacks	CAVs Log Files Preservation	CAV's network observability is primarily based on log files. All CAV activities in ITS are documented in log files. Cyber-assaults - valuable input to log file preservation - can serve as lessons learned and aid in investigating hacker attacks and motivations.	Medium	+	(Dimitriadis et al., 2020)
CAVs Log Files Preservation	CAVs Technology Readiness and Maturity	Retaining log files for all CAVs interactions for a specified period would improve ITS reliability, protect CAVs cybersecurity posture of cloud computing environments, and enhance CAVs decision-making	Medium	+	(Prasad and Rohokale, 2020)
CAVs Technology Readiness and Maturity (TRM)	CAVs Communication Cyber Safety (CAVS-CCS)	TRM, which assesses the communication framework of CAVs and demonstrates its capabilities, is triggered by the level of technology, procedures, qualified personnel and information. Defence Science and Technology Group in Australia spotlighted	Medium	+	(Vimmerstedt et al., 2015, Australia-Goverment,

		the nine-level of estimating the maturity of technologies during the acquisition phase. Innovation in technology maturity will lead to more secured V2X communication.			2020, Khan et al., 2021c).
CAVs Communication Cyber Safety (CAVs-CCS)	Hacks defended	A highly robust CAVs communication framework is less vulnerable to attacks and is incredibly difficult for hackers to infiltrate. Additionally, Unnamed Aerial Vehicles may function as an ad-hoc, cost-effective telecommunications network, allowing CAVs to communicate in mountainous or dark regions. For instance, the use of UAVs in conjunction with 5G networks, both for access and backhaul,	High	+	(Khan et al., 2020d, Khan et al., 2020c, Khan et al., 2020b, Khan et al., 2020a, Khan, 2020, Khan, 2019, Khan et al., 2019)

Figure 1: The system architecture of the Causal Loop Diagram (CLD).



4. Model Qualitative Analysis: Loops and System archetype.

CLDs coherently conceptualise dynamic systems to facilitate understanding of interdependencies of R&PF in CAVs cybersecurity framework. The loops envision a "system archetype" that disclose inherent limitations within the system by identifying intervention opportunities, allowing policy recommendations to be developed appropriately (Sterman, 2000). The following sub-sections describe various feedback loops and system archetype.

4.1 Balancing Loop #1

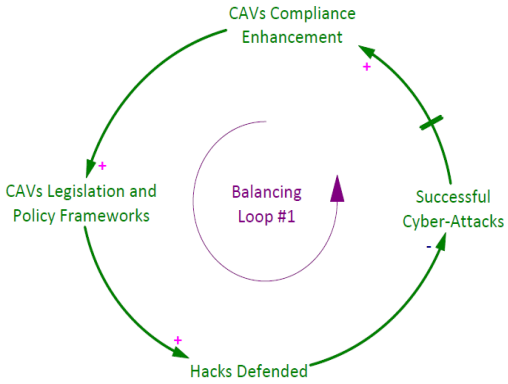
Figure 2a depicts the balancing loop #1 in which policy readiness, regulation/laws readiness, liability readiness, CAVs criminology-theory maturity, and the eSafety Traffic Unit reinforce CAVs compliance enhancement. This loop describes the mechanism of how governments

combat the perceived cybersecurity threat posed by hackers by refining the R&PF and, as a result, increasing the number of hacks defended.

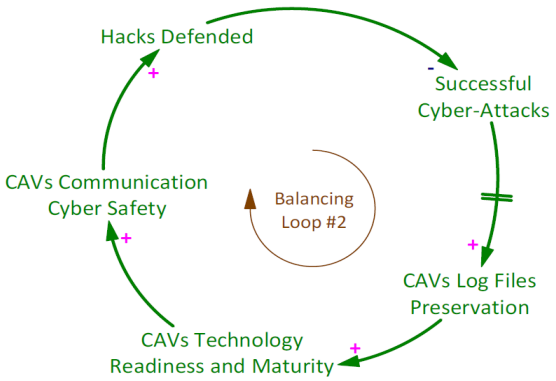
4.2 Balancing Loop #2

Similarly, balancing loop #2 is shown in Figure 2b. Successful cyber-attacks are stored as log files- a valuable input for CAVs TRM and CAVs-CCS. This, in turn, makes it possible for a large number of successfully defended hacks. Alternatively, less knowledge of a hacker's capability reduces the capacity to fight against hackers, resulting in a greater rate of successful assaults.

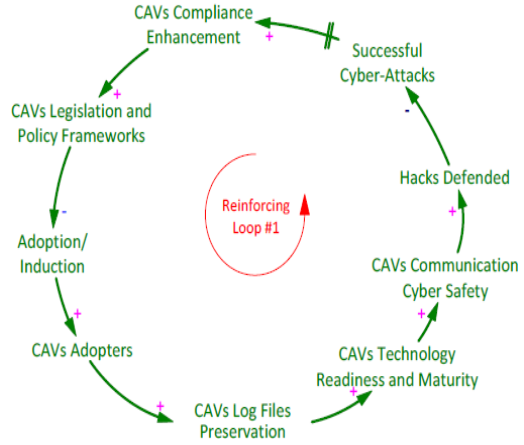
Figure 2: Feedback loops in CLD



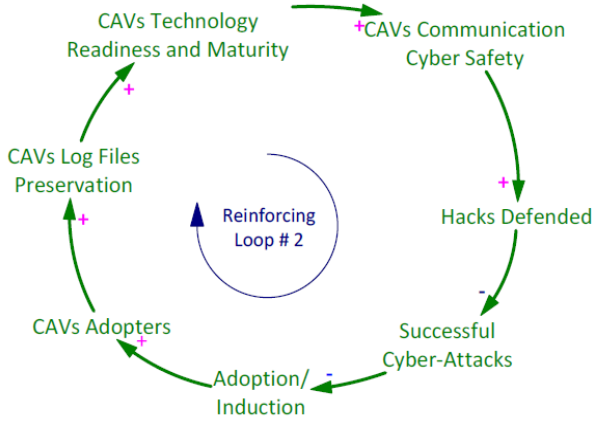
a. Balancing loop #1



b. Balancing loop #2



c. Reinforcing loop #1



d. Reinforcing Loop #2

4.3 Reinforcing Loop #1

Figure 2c illustrates reinforcing loop #1. This loop explains how prospective CAV users view the R&PF actions as impeding their freedom. As a result, users respond by decreasing imitation, slowing the adoption and induction of CAVs adaptors and log file preservation. Consequently, CAVs-CCS is hampered.

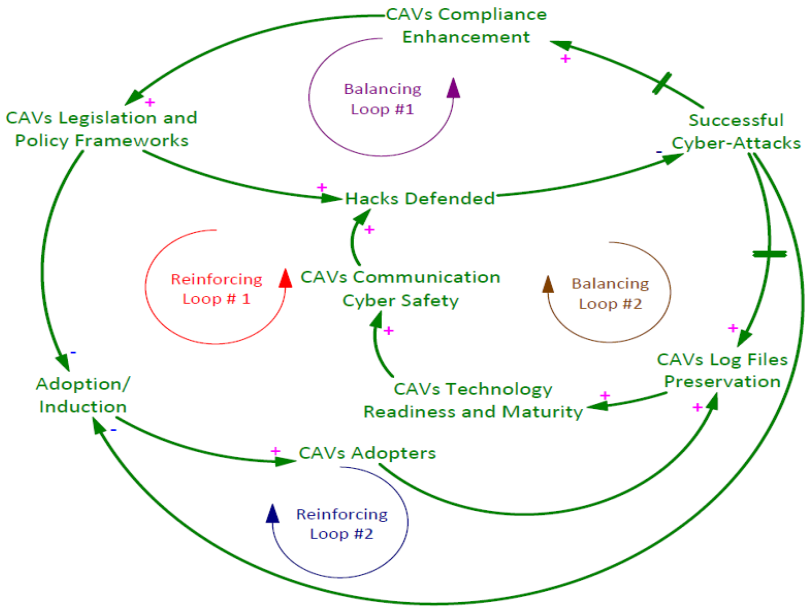
4.4 Reinforcing Loop #2

The reinforcing loop#2 is shown in Figure 2d. This loop demonstrates how successful cyberattacks decrease CAVs adoption and induction. This may impede the CAVs TRM, CAVs-CCS, as well as, hacks defended.

4.5 Holistic View: Shifting the burden-system archetype

The loops envisage system archetype that reveals underlying system limits by highlighting intervention prospects. Figure 3 depicts a holistic view and is analogous to the "shifting the burden" archetype. Decision-makers in the "shifting the burden" archetype fail to find the fundamental answer early on and are exposed to cumulative adverse effects as they turn to short corrective measures. This explains the process by which governments respond to perceived cybersecurity threats by strengthening R&PF; consumers and OEMs view this activity as restricting their freedom.

Figure 3: Holistic view- "shifting the burden" system archetype



5. Discussions and policy recommendations

This article aims to illustrate the potential pitfalls of decision-making (R&PF) in governing a complex and dynamic system, i.e., CAV-based ITS. An approach to dealing with a complicated decision-making system is to recognise general structures referred to as systems archetypes. The idea underlying system archetypes is that undesirable outcomes or side effects may be linked to common behavioural patterns. The development of a CLD-based SD model for assessing the impact of R&PF on the cybersecurity of CAVs is a significant contribution because it provides a dynamic, interconnected view of the "big picture".

The balancing loops #1 and 2 illustrate how effective R&PF can thwart cyber-attacks with the help of policy readiness, regulation/laws readiness, liability readiness, CAVs, criminology-theory maturity, and the eSafety Traffic Unit. Reinforcing loops #1and 2, on the other hand, demonstrate how a change in one direction is exacerbated by further change. Decision-makers should proactively identify these potential hazards: CLD-based SD models can assist in this endeavour and provide an environment to simulate various decision situations. For instance, what could a pitfall avoidance strategy in R&PF be that does not impair the freedom of CAV users, investors and automakers?

The R&PF of CAVs would have an effect on a variety of aspects, including data security and privacy, short-term economic considerations, public infrastructure, and social and economic dimensions (He, 2018, Khan et al., 2020e, Seuwou et al., 2020). The complexity of the ITS

grows as more CAVs are deployed. While the R&PF for CAVs establishes safe operating limits for CAVs, it is essential to formulate the R&PF with a measured and risk-adjusted approach to avoid the repercussions described in reinforcing loops #1 and #2.

The most challenging matter in this context is determining the trade-off between the three components: i) constraints on CAV users' privacy and freedom, ii) operational and data accessibility limitations for CAV OEMs and service providers as well as protection of their business investments, and iii) command and control limits for state regulators. Nevertheless, some of the R&PF will be driven by real-world reasoning in courts, following the submission of a typical CAV-related incident for adjudication.

6. Limitations and future extensions

Although the suggested model incorporates an in-depth, methodical, and rigorous approach, it does have certain confines. Data scarcity, a high degree of uncertainty, and the subjectivity nature of R&PF make the model's empirical assessment challenging. Therefore, the following steps could be data collection for quantitative evaluation of the model. The primary source will be a survey conducted with the appropriate field specialists, aided by pilot programmes such as "Austroads Future Vehicles & Technology Program" in Australia (Austroads, 2021; Vicroads, 2021). On the other hand, qualitative research may remain the dominant option for a few years longer until an adequate amount of data becomes available.

7. Conclusions

This paper proposed a CLD-based SD model that incorporates key inter-disciplinary variables and evaluates the impact of R&PF on CAVs cybersecurity in a dynamic and integrated manner. Two loops are envisaged: "balancing loops" highlight instances where R&PF aid in preventing cyber-attacks, and "reinforcing loops" reveal how imposing R&FP can offset its potential benefits by creating a detrimental parallel circle. Based on feedback loops, a "shifting the burden" system archetype is proposed in which governments counter cyber-threats by boosting R&PF while also decreasing CAVs adaptability through imitation and induction. Recommendations for R&PF formulation include a balanced approach in the trade-off between: i) constraints on CAV users' privacy and freedom, ii) operational and data accessibility limitations for CAV OEMs and service providers, and iii) command and control limits for state regulators.

References

Australia-Goverment (2020) Technology Readiness Level Definition. *Defence Science and Technology Group* **https://www.dst.defence.gov.au/sites/default/files/basic_pages/documents/TRL%20Explanations_1.pdf**.

Bass, F. M. (1969) A new product growth for model consumer durables. *Management science* **15(5)**:215-227.

Cabinet Office (2016) National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP. *National cyber security strategy 2016–2021.* **https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021**.

Dimitriadis, A., Ivezic, N., Kulvatunyou, B. & Mavridis, I. (2020) D4I-Digital forensics framework for reviewing and investigating cyber attacks. *Array* **5**:100015.

Dosen, I., Aroozoo, M. & Graham, M. (2017) *Automated vehicles.* Parliament Library & Information Service, Parliament of Victoria.

Elzen, B., Geels, F. W. & Green, K. (2004) *System innovation and the transition to sustainability: theory, evidence and policy.* Edward Elgar Publishing.
Feng, S., Feng, Y., Yan, X., Shen, S., Xu, S. & Liu, H. X. (2020) Safety assessment of highly automated driving systems in test tracks: A new framework. *Accident Analysis & Prevention* **144**:105664.
Forrester, J. W. (1958) Industrial Dynamics. A major breakthrough for decision makers. *Harvard business review* **36(4)**:37-66.
Geels, F. W. & Penna, C. C. (2015) Societal problems and industry reorientation: Elaborating the Dialectic Issue LifeCycle (DILC) model and a case study of car safety in the USA (1900–1995). *Research Policy* **44(1)**:67-82.
Haratsis, B., Carmichael, T., Courtney, M. & Fong, J. (2018) Autonomous vehicles employment impact study.), vol. https://advi.org.au/media-centre/autonomous-vehicles-employment-impact-report/.
He, H. (2018) Cybersecurity law causing "mass concerns" among foreign firms in China. *South China Morning Post* **https://www.scmp.com/news/china/economy/article/2135338/cybersecurity-law-causing-mass-concerns-among-foreign-firms-china**.
Hodge, C., Hauck, K., Gupta, S. & Bennett, J. C. (2019) *Vehicle Cybersecurity Threats and Mitigation Approaches*.
Johnson, C. (2017) Readiness of the road network for connected and autonomous vehicles. *RAC Foundation: London, UK*.
Khan, S. K. (2019) Performance evaluation of next generation wireless UAV relay with millimeter-wave in access and backhaul. *Master Thesis, School of Engineering, RMIT University, Melbourne, Australia*.
Khan, S. K. (2020) Mathematical framework for 5G-UAV relay. *Transactions on Emerging Telecommunications Technologies*
e4194.
Khan, S. K., Al-Hourani, A. & Chavez, K. G. (2020a) Performance Evaluation of Amplify-and-Forward UAV Relay in Millimeter-Wave. In *2020 27th International Conference on Telecommunications (ICT)*.) IEEE, pp. 1-5.
Khan, S. K., Farasat, M., Naseem, U. & Ali, F. (2019) Link-level Performance Modelling for Next-Generation UAV Relay with Millimetre-Wave Simultaneously in Access and Backhaul. *Indian Journal of Science Technology* **12(39)**:1-9.
Khan, S. K., Farasat, M., Naseem, U. & Ali, F. (2020b) Performance evaluation of next-generation wireless (5G) UAV relay. *Wireless Personal Communications* **113(2)**:945-960.
Khan, S. K., Naseem, U., Sattar, A., Waheed, N., Mir, A., Qazi, A. & Ismail, M. (2020c) UAV-aided 5G Network in Suburban, Urban, Dense Urban, and High-rise Urban Environments. In *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*.) IEEE, pp. 1-4.
Khan, S. K., Naseem, U., Siraj, H., Razzak, I. & Imran, M. (2020d) The role of unmanned aerial vehicles and mmWave in 5G: Recent advances and challenges. *Transactions on Emerging Telecommunications Technologies*:e4241.
Khan, S. K., Shiwakoti, N. & Stasinopoulos, P. (2021a) A Conceptual System Dynamics Model for Cybersecurity Assessment of Connected and Autonomous Vehicles. *Accident Analysis & Prevention*.
Khan, S. K., Shiwakoti, N. & Stasinopoulos, P. (2021b) Modelling Cybersecurity in Connected and Autonomous Vehicles *Accident Analysis & Prevention*.
Khan, S. K., Shiwakoti, N. & Stasinopoulos, P. (2021c) Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks In *Proceedings of 2021 International Symposium on Connected and Autonomous Vehicles (SoCAV 2021)* vol. Accepted.
Khan, S. K., Shiwakoti, N., Stasinopoulos, P. & Chen, Y. (2020e) Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention* **148**:105837.

Lederman, J., Garrett, M. & Taylor, B. D. (2016) Fault-y reasoning: navigating the liability terrain in intelligent transportation systems. *Public Works Management Policy* **21(1)**:5-27.

Liu, N., Nikitas, A. & Parkinson, S. (2020) Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation Research Part F: Traffic Psychology Behaviour* **75**:66-86.

Mewton, R. (2005) Induced traffic from the Sydney Harbour Tunnel and Gore Hill Freeway. *Road Transport Research* **14(3)**:24.

Newton, A. (2017) Crime, transport and technology. In *The Routledge Handbook of Technology, Crime and Justice*.) Routledge, pp. 281-294.

Nieuwenhuijsen, J., De Almeida Correia, G. H., Milakis, D., Van Arem, B. & Van Daalen, E. (2018) Towards a quantitative method to analyze the long-term innovation diffusion of automated vehicles technology using system dynamics. *Transportation Research Part C: Emerging Technologies* **86**:300-327.

Noy, I. Y., Shinar, D. & Horrey, W. J. (2018) Automated driving: Safety blind spots. *Safety science* **102**:68-78.

Prasad, R. & Rohokale, V. (2020) *Cyber Security: The Lifeline of Information and Communication Technology*. Springer.

Rosique, F., Navarro, P. J., Fernández, C. & Padilla, A. (2019) A systematic review of perception system and simulators for autonomous vehicles research. *Sensors* **19(3)**:648.

Sae-International (2018) Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles.

Seuwou, P., Banissi, E. & Ubakanma, G. (2020) The Future of Mobility with Connected and Autonomous Vehicles in Smart Cities. In *Digital Twin Technologies and Smart Cities*.) Springer, pp. 37-52.

Stanford, J. (2015) Possible futures for fully automated vehicles: using scenario planning and system dynamics to grapple with uncertainty.) Massachusetts Institute of Technology.

Stasinopoulos, P., Shiwakoti, N. & Beining, M. (2020) Use-Stage life cycle Greenhouse Gas Emissions of the Transition to an Autonomous Vehicle Fleet: A System Dynamics approach. *Journal of Cleaner Production*:123447.

Sterman, J. (2000) Business Dynamics: Systems Thinking and Modeling for a Complex World McGraw Hill NY.

Taeihagh, A. & Lim, H. S. M. (2019) Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews* **39(1)**:103-128.

Uzair, M. (2021) Who Is Liable When a Driverless Car Crashes? *World Electric Vehicle Journal* **12(2)**:62.

Vimmerstedt, L. J., Bush, B. W. & Peterson, S. O. (2015) *Dynamic modeling of learning in emerging energy industries: The example of advanced biofuels in the United States*.

Williams, E., Das, V. & Fisher, A. (2020) Assessing the Sustainability Implications of Autonomous Vehicles: Recommendations for Research Community Practice. *Sustainability* **12(5)**:1902.