TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 4
December 2025
DOI: 10.12716/1001.19.04.19

Cybersecurity Breaches in Connected and Autonomous Vehicles: Rethinking Liability and Insurance Frameworks

A.H.M. Abuelenin
King Abdulaziz University, Jeddah, Saudi Arabia

ABSTRACT: As connected and autonomous vehicles (CAVs) become integrated into modern transport systems, cybersecurity vulnerabilities pose significant legal and regulatory challenges. This paper examines the consequences of large-scale hacking incidents involving CAVs, where software compromise may lead to accidents, injury, or loss. Current insurance and liability regimes are ill-equipped to address the complexities of mass-risk events triggered by cyberattacks. Drawing from the United Kingdom's Automated and Electric Vehicles Act 2018 and broader European frameworks, we identify critical gaps in existing legislation. We propose a reformed insurance model that includes a national compensatory body or reinsurance pool to ensure equitable redress for third-party victims. Our findings offer broader insights for regulatory design in the maritime sector, where cybersecurity threats to safety-critical systems demand proactive legal responses.

1 INTRODUCTION

Connected and autonomous vehicles (CAVs) are a cornerstone of emerging intelligent transport systems, with wide-ranging implications across land, maritime, and aviation sectors. Their development promises reductions in road accidents, improved traffic efficiency, and environmental benefits. However, the convergence of artificial intelligence, digital connectivity, and vehicle automation also introduces profound cybersecurity vulnerabilities. These risks are especially pronounced in the context of software-dependent systems capable of operating without direct human control, where cyberattacks could lead to physical harm, infrastructure disruption, and systemic failures across fleets operating on common platforms.

While the integration of CAVs into public and private transport networks accelerates, legal and insurance regimes have struggled to adapt to the unique challenges of cybersecurity breaches. These include not only the immediate physical consequences of a compromised vehicle but also the complex question of liability attribution when the harm results from intentional third-party hacking. Notably, CAVs are vulnerable to wireless cyber intrusions, allowing attackers to remotely manipulate operational systems without requiring physical access [1; 2; 3]. The use of uniform software across fleets increases the likelihood of mass-risk events, where multiple vehicles may be simultaneously exploited—an issue not fully addressed in current regulatory or insurance frameworks [4; 5].

Although discussions around CAV safety and liability have been progressing, particularly in engineering and legal communities [6; 7], the specific issue of liability for cybersecurity breaches remains underdeveloped in both scholarship and statute [4; 8]. Existing models of insurance and product liability, such as those based on the UK's Road Traffic Act 1988 and the Consumer Protection Act 1987, are not well

suited for attributing responsibility in scenarios involving deliberate cyberattacks. In traditional road traffic incidents, third-party victims are typically compensated through insurance or by the Motor Insurers' Bureau (MIB) when the responsible party is untraced or uninsured [9; 10]. However, these schemes may be ineffective where the cause is digital, distributed, and perpetrated anonymously, challenging both fault attribution and policy applicability [11].

The United Kingdom's Automated and Electric Vehicles Act 2018 (AEVA) is among the first attempts to address some of these gaps. It mandates that insurers compensate victims of accidents involving automated vehicles when "driving itself" [12]. This strict liability model—requiring no proof of negligence or product defect—aims to ensure swift redress. Yet, the Act does not clearly resolve how cybersecurity-related incidents fit within its framework. Questions remain as to whether vehicles under malicious third-party control are considered to be "driving themselves" and whether insurers can exclude liability when safety-critical software updates have not been applied [13].

Additionally, product liability law as applied to software remains unsettled. While physical software media may qualify as "products" under the CPA 1987, over-the-air updates may not [14; 15; 16]. The absence of consensus around software defectiveness, coupled with defenses like the "state-of-the-art" or development risk defense [17; 18], may leave insurers and manufacturers locked in costly legal disputes while victims await compensation [19; 20]. This uncertainty could have broader implications beyond CAVs, particularly in the maritime sector, where autonomous ships and port systems also face growing cybersecurity threats [21; 22].

To mitigate these risks, this paper argues for the establishment of a national compensatory mechanism, akin to the MIB or the UK's Flood Re scheme, to ensure that victims of CAV-related cyberattacks are not left without remedy. This framework would function as a reinsurance pool or guarantee fund, distributing risk across manufacturers and insurers while promoting innovation without sacrificing consumer protection [4; 23]. The broader objective is to provide legal certainty and financial resilience not only for CAV users but for the wider autonomous transport ecosystem—an imperative shared by maritime policy actors contending with similar vulnerabilities in critical safety systems [21; 22].

2 LITERATURE REVIEW

2.1 *Cyber Risk in Connected and Autonomous Vehicles*

The integration of digital technologies into vehicle design has transformed connected and autonomous vehicles (CAVs) into mobile computing systems with embedded software, real-time data exchange capabilities, and remote connectivity. This interconnectedness significantly elevates the cyber threat profile of CAVs, rendering them attractive targets for malicious actors. Unlike conventional vehicles, CAVs are susceptible to attacks through wireless networks, allowing unauthorized access to critical systems without physical contact. The ramifications of such breaches extend beyond mere data theft; they encompass loss of vehicle control, physical collisions, and coordinated disruption across entire fleets [1; 2].

Hacking vulnerabilities in CAVs are not confined to theoretical speculation. Real-world demonstrations and academic studies have shown that attackers can exploit sensor manipulation, spoofing of vehicle-to-infrastructure (V2I) communication, and remote code injection to compromise operational integrity [5; 24]. The cyber-physical nature of CAVs means that breaches can directly endanger human life and property. In high-density urban settings or constrained transport environments—such as port access corridors—such vulnerabilities could cause cascading failures with wide-ranging socioeconomic consequences. Moreover, AI-driven functionalities embedded in CAVs may amplify these risks, given the unpredictability of machine learning models when faced with adversarial inputs [3; 21].

Mass hacking events pose particular concerns. As software in CAVs is often standardized across entire model lines or fleets, a single vulnerability can affect thousands of vehicles simultaneously. In such scenarios, attackers could manipulate traffic systems, disable safety features, or trigger collisions en masse. The challenge is further compounded by over-the-air software updates, which, while necessary for maintaining system integrity, also present a potential attack vector if authentication protocols are flawed [25; 26]. These risks are not unique to land transport systems; autonomous vessels, drones, and smart port infrastructure share similar vulnerabilities, underscoring the cross-sector importance of effective cyber resilience strategies [21; 22].

The dynamic and evolving nature of cybersecurity threats makes regulatory and legal preparedness particularly difficult. Although cybersecurity guidance for manufacturers exists—such as the UK's Key Principles of Vehicle Cyber Security and UN recommendations on over-the-air update security—compliance remains voluntary and enforcement mechanisms are limited [27; 25]. This creates uncertainty not only for end-users but also for insurers, regulators, and third-party victims. Notably, while maritime systems may benefit from industry-specific cybersecurity standards (e.g., IMO's guidelines for maritime cyber risk management), a harmonized cross-sectoral framework is still lacking, particularly where land and sea transport intersect through logistics hubs and automated freight systems.

One of the most critical issues is the lack of clear liability allocation following a cyber breach. As identified in UK law commission reports and legal commentary, hacking scenarios often fall outside the scope of existing tort or product liability frameworks, making redress difficult [4; 15]. In maritime contexts, similar gaps exist in terms of responsibility for cyber-induced navigational failures or port-side accidents. Whether the fault lies with software developers, component manufacturers, fleet operators, or vehicle owners is rarely straightforward. The difficulty in tracing cyberattacks, coupled with the growing sophistication of hacking methods, raises the

possibility of victims being left uncompensated in the absence of a robust insurance or guarantee fund [23].

Finally, cybersecurity breaches may trigger broader systemic risks. The public's trust in autonomous systems hinges not only on their mechanical and navigational safety but also on their resistance to malicious interference. Without confidence in the integrity and accountability of CAV operations, consumer uptake may falter, undermining the policy goals of reducing traffic fatalities and emissions. Moreover, for marine policy stakeholders, these challenges are instructive: as vessels, ports, and logistics chains become increasingly digitized and autonomous, the threat landscape observed in CAVs provides a useful model for anticipating regulatory shortcomings in other transport modalities.

2.2 *Comparative Sectoral Insights: Lessons from Maritime and Aviation Cybersecurity*

The vulnerabilities exposed in CAVs offer critical lessons for other safety-critical sectors undergoing digital transformation, particularly maritime and aviation systems. While the legal and insurance frameworks surrounding CAV cybersecurity remain fragmented, similar regulatory ambiguities exist in the governance of autonomous maritime technologies, port infrastructure, and unmanned aircraft. Each sector faces the challenge of adapting traditional liability regimes to a digital risk landscape marked by anonymity, software complexity, and potential mass failure.

In the maritime context, unmanned ships and connected port systems have become targets for cyberattacks capable of disrupting navigation, supply chains, and onboard safety systems [21; 22]. Recent real-world initiatives illustrate the growing adoption of MASS technologies and highlight the cybersecurity challenges they face. For example, the Norwegian ferry Yara Birkeland is often cited as the world's first fully electric and autonomous cargo ship, operating with minimal human oversight while navigating coastal waters. Similarly, Japan's NYK Line has conducted autonomous ship trials under the MEGURI2040 project, aiming to commercialize autonomous vessels by 2025. The European Union's AUTOSHIP project also seeks to develop and test autonomous cargo ships and port operations across the North Sea region. These examples demonstrate that MASS technologies are no longer theoretical; however, they also expose vulnerabilities related to cyber intrusion and liability uncertainty, mirroring concerns already seen in CAV cybersecurity debates.

The broad range of technical failures—spanning GPS spoofing, automated route manipulation, and remote disabling—raises difficult questions about liability division between vessel owners, manufacturers, and third-party service providers. Notably, maritime law's existing provisions on seaworthiness and fault-based liability do not adequately account for cyber-induced operational failure, especially when software updates and cybersecurity fall outside the operator's control [21]. In the event of damage or loss, victims may struggle to recover compensation unless the responsible actor can be clearly identified—a challenge echoed in CAV hacking incidents.

Aviation systems, while more centralized and regulated, are also susceptible to cyber threats. Remotely piloted aircraft and automated air traffic systems are increasingly reliant on secure data transmission and embedded software logic. Similar to CAVs, these systems may suffer from undetectable vulnerabilities until exploited, leaving legal uncertainty over fault attribution [26]. In both sectors, the involvement of multiple component suppliers and service vendors complicates the application of product liability and negligence doctrines. This creates exposure gaps where damage arises not from conventional equipment failure but from software manipulation or network intrusion.

Efforts in maritime and aviation governance to develop cybersecurity protocols—such as the IMO's guidelines and ICAO frameworks—illustrate the value of proactive, sector-specific standards. However, these efforts often stop short of establishing clear liability and compensation mechanisms, especially in cross-jurisdictional scenarios. The legal grey areas faced by CAVs thus reflect broader systemic challenges across autonomous transport ecosystems. Policymakers and insurers should consider interoperable compensatory structures, such as guarantee funds or no-fault schemes, that can be adapted across sectors to mitigate mass cyber risks and support public trust in increasingly autonomous systems [4; 23].

2.3 *Existing Liability and Insurance Models*

Legal and insurance frameworks for managing risks in connected and autonomous systems have traditionally evolved from models built around fault-based principles, such as negligence and product liability. In the context of CAVs, however, these models face significant limitations when applied to cybersecurity breaches. Central to these limitations is the challenge of causation: when malicious third parties intervene via remote hacking, tracing responsibility back to a manufacturer, software developer, or vehicle owner becomes increasingly complex [4; 8].

In the UK, the Road Traffic Act 1988 mandates compulsory third-party motor insurance, supplemented by the MIB, which compensates victims of uninsured or untraced drivers [9]. While effective in traditional motor vehicle contexts, these mechanisms are not designed to address harms caused by mass cyber incidents involving no identifiable human driver. Likewise, the AEVA introduces a strict liability scheme for insurers, requiring them to compensate victims where a vehicle is operating in "automated mode," regardless of driver fault [12]. This regime increases certainty for victims but does not resolve the complexities of recourse for insurers seeking indemnification from manufacturers or software providers—particularly when over-the-air updates or remote vulnerabilities are implicated [12; 20].

Product liability law, particularly under the UK's Consumer Protection Act 1987, may offer insurers a potential avenue for recourse. However, uncertainties persist regarding the legal status of software as a "product," especially where updates are delivered digitally rather than on physical media [14; 15; 16].

Additionally, defences such as the "development risk" clause allow manufacturers to escape liability if the defect was undiscoverable given the state of scientific and technical knowledge at the time [17]. These limitations place the burden of compensation primarily on insurers, despite their limited ability to control software design or cybersecurity standards.

Moreover, in practical terms, this legal uncertainty often results in significant delays for victims seeking compensation. Insurers, wary of the difficulty in securing indemnification from manufacturers or software suppliers, may either limit policy coverage or pursue prolonged litigation to apportion costs. For example, where a cybersecurity breach stems from an undetected software flaw later exploited through a remote update, insurers must navigate complex evidentiary burdens to establish fault, frequently involving technical forensic investigations and multi-jurisdictional discovery processes. These hurdles not only prolong redress for injured parties but also increase overall claims costs, discouraging proactive market engagement in underwriting cyber risks for autonomous systems.

Maritime insurance frameworks face similar issues when confronted with automation and cyber risk. Conventional marine policies focus on physical loss or navigational fault and are ill-suited to address systemic failures caused by malware or network compromise. This reinforces the need for revising liability allocation and risk-sharing mechanisms across autonomous transport sectors, especially as cyber-physical systems become foundational to modern transport infrastructure [21; 22; 23].

2.4 *The Automated and Electric Vehicles Act 2018*

The UK's Automated and Electric Vehicles Act 2018 (AEVA) represents a significant legislative effort to modernize insurance in response to the advent of autonomous technologies. Central to the Act is the establishment of a first-party insurance framework that requires insurers to compensate victims where an automated vehicle is "driving itself," removing the need for fault attribution or product defect proof [12]. The Act thus offers a strict liability model that aims to ensure prompt redress following incidents involving automated systems, including those potentially caused by cybersecurity breaches.

The AEVA introduces critical terminology, notably the requirement that a vehicle be listed as "capable of driving itself safely" for coverage to apply [12]. However, ambiguity persists around the definition of "driving itself" in scenarios involving cyberattacks. According to section 8, a vehicle is considered autonomous only when not being controlled or monitored by an individual. This becomes problematic when a hacker seizes control, creating uncertainty over whether the vehicle meets the threshold for automated operation under the Act [28; 29].

The Act also attempts to manage risk through limited exclusions. Insurers may deny or recover compensation from the policyholder if software updates deemed "safety critical" were knowingly ignored, or if unauthorized modifications were made [12; 13]. While this provision aims to incentivize safe user behavior, it assumes a level of technical understanding that may be unrealistic for lay vehicle owners. Moreover, failure to apply an update could arguably reflect a manufacturer's oversight if adequate warnings were not provided, introducing the possibility of a product liability counterclaim [30].

AEVA's attempt to clarify insurance obligations is a notable legal development, yet its effectiveness in addressing cybersecurity liability is constrained. The law does not define what constitutes a cyber-safe vehicle or establish standards for resilience against digital intrusion. This legislative silence risks creating uneven implementation and disputes between insurers and manufacturers over liability and indemnity. Such challenges parallel those observed in maritime law, where cyber resilience expectations are not yet codified into enforceable insurance or liability norms [21; 22].

As autonomous systems grow in complexity across sectors, AEVA's principles may serve as a policy prototype. However, for broader applicability—including in marine contexts—legal clarity around digital threats, third-party interference, and system integrity will be essential for building resilient, fair liability regimes.

2.5 *Gaps in Current Legal and Insurance Frameworks*

Despite recent advancements in autonomous vehicle legislation, key gaps remain in the legal and insurance frameworks that govern cybersecurity risks. These gaps are particularly critical when malicious third-party interference causes system failure, raising concerns about redress, accountability, and resilience across sectors reliant on automated technologies.

A major shortcoming is the lack of clarity in liability attribution when damage results from mass hacking. The interplay between product liability, insurance, and end-user responsibility becomes opaque, especially when software vulnerabilities are exploited without the knowledge or action of the vehicle owner [4; 8; 23]. Insurers, although obligated to compensate under laws like the AEVA 2018, face uncertainty in recovering costs from manufacturers due to unresolved questions around software defectiveness and "state-of-the-art" defences [18].

Compounding this is the inconsistent treatment of software as a legal product. While embedded systems may fall within product liability statutes, over-the-air updates and cloud-based functionalities often remain outside traditional legal definitions, leaving open questions about when liability is triggered and by whom [14; 15; 16]. This lack of legal consensus hinders both insurers and victims from pursuing effective claims.

Maritime systems face similar uncertainties. While sectors recognize cybersecurity as a strategic concern, their legal regimes remain reactive rather than anticipatory. The absence of binding norms for attributing responsibility in cyber-related incidents mirrors the dilemmas observed in CAV governance, where insurance and liability mechanisms lag behind technological realities [21; 22]. Without harmonized legal definitions of digital safety, control, and responsibility, victims of autonomous system failures—whether on roads, seas, or in the air—may find themselves in a "liability vacuum." This exposes

systemic weaknesses that undermine public confidence and delay the safe integration of autonomous technologies.

In addition to frameworks like the AEVA and traditional product liability models, several jurisdictions are beginning to recognize the need for policies explicitly addressing liability in mass-risk cyber incidents involving autonomous systems. For example, in the United States, proposals such as the SELF DRIVE Act emphasize federal safety standards for highly automated vehicles but leave significant gaps regarding mass cyberattack liability, leading some scholars to advocate for national compensation funds similar to the Terrorism Risk Insurance Program (TRIP). In Japan, the government's efforts under the Strategic Innovation Promotion Program (SIP-adus) include research into insurance frameworks that would cover mass hacking incidents affecting multiple vehicles simultaneously. Singapore has introduced mandatory insurance requirements for autonomous vehicle testing that contemplate aggregated risk scenarios, although permanent policies are still evolving. Notably, Australia's National Transport Commission has also recommended developing automated vehicle insurance schemes that would extend beyond individual accidents to account for systemic failures, including cyberattacks. These emerging approaches underscore the urgent need to supplement individual accident liability models with collective risk-sharing mechanisms, such as reinsurance pools, no-fault compensation schemes, and publicly backed funds to ensure that victims of mass cybersecurity events are swiftly and fairly compensated.

3 METHODOLOGY

3.1 *Legal-Doctrinal Approach*

This research adopts a legal-doctrinal approach to examine how current liability and insurance frameworks respond to cybersecurity breaches in CAVs, with comparative relevance to similarly vulnerable maritime and aviation systems. The doctrinal method focuses on the critical analysis of legal texts, case law, statutory instruments, and policy frameworks, aiming to interpret and evaluate existing legal doctrines in light of technological advancements and emerging risk landscapes.

Primary sources of law examined include the AEVA and the Road Traffic Act 1988, along with foundational documents related to product liability, such as the Consumer Protection Act 1987. These instruments are evaluated for their capacity to address incidents involving mass hacking, software manipulation, and the resulting physical and economic harm. Central to this evaluation is the interpretation of terms such as "accident," "driving itself," and "safety critical," which carry significant weight in determining the applicability and limits of statutory protections [12; 13].

The analysis also incorporates relevant case law that sheds light on the scope of insurance liability and fault attribution, particularly in cases where damages arise from intentional or unforeseen external interference. For instance, Hardy v MIB and Bristol Alliance v Williams demonstrate the courts' protective stance towards third-party victims, emphasizing that compensation should be available even in cases of deliberate or criminal conduct [31; 32].

Secondary sources—including legal commentary, academic literature, and regulatory reports—are used to contextualize doctrinal interpretation within broader policy debates [15]. Insights are further drawn from the work of scholars who analyze liability extensions into the software domain, particularly regarding whether over-the-air updates constitute "products" for the purpose of strict liability regimes [14; 15; 16].

The doctrinal approach is especially relevant to marine policy, where regulatory fragmentation and jurisdictional complexity are common. By analyzing how the UK and EU legal systems attempt to integrate cyber risk into traditional insurance and liability models, this study provides a blueprint for addressing parallel gaps in maritime law. The methodology thus enables critical reflection on how doctrinal rigidity may hinder effective governance in the face of digitization, offering a foundation for legislative and institutional reform across automated transport domains [21; 22].

3.2 *Policy Evaluation Framework*

Complementing the legal-doctrinal approach, this study applies a structured policy evaluation framework to assess the adequacy of existing and proposed insurance and liability mechanisms in managing cybersecurity risks in autonomous systems. The evaluation draws upon regulatory analysis and comparative institutional insights, focusing on how legal regimes respond to complex, multi-actor cyber threats that transcend conventional boundaries of risk attribution.

The framework prioritizes three core criteria: (1) victim compensation and access to justice; (2) the effectiveness of insurer and manufacturer responsibility-sharing; and (3) the resilience of institutional structures under mass-risk scenarios. These criteria are applied to the AEVA, the traditional UK motor insurance regime under the Road Traffic Act 1988, and the MIB agreements [9; 10; 12].

Particular emphasis is placed on evaluating how well current policies align with the reality of software-driven risk and digital system failure. The framework examines the absence of clear obligations for cybersecurity compliance, the ambiguity surrounding software liability under product law, and the limitations of insurer recovery rights when software is deemed the primary cause of loss [14; 18; 23]. These shortcomings are assessed against the broader goal of public risk mitigation, considering parallels with other sectors such as autonomous shipping, where institutional fragmentation similarly impairs proactive governance [21; 22].

Through this evaluation, the study explores whether alternative models—such as reinsurance pools or central guarantee funds—could offer more equitable and efficient outcomes. The analysis serves to inform future marine policy, where such models may be adapted to address the growing threat landscape associated with autonomous maritime operations and cyber-physical integration.

3.3 *Justification for Focus on UK and EU Jurisdictions*

This study focuses primarily on the legal and policy frameworks of the United Kingdom and the European Union, where legislative developments around CAVs and cybersecurity liability are among the most advanced globally. The UK's AEVA and the EU's Regulation (EU) 2019/2144 on vehicle safety provide early examples of attempts to reconcile traditional liability models with the evolving risks posed by autonomous technologies [33; 12].

The UK was among the first jurisdictions to legislate explicitly for CAV insurance liability, positioning AEVA as a key instrument for evaluating the legal treatment of automation-related harm. The Act introduces strict liability mechanisms, limited insurer exclusions, and recourse options that are particularly useful for comparative analysis in both land and maritime contexts [12; 13]. Meanwhile, EU legislation has focused on mandatory safety features and cybersecurity compliance, but questions remain over harmonized enforcement and clarity in liability attribution [33; 18].

The choice of these jurisdictions also reflects their strong institutional engagement with cyber risk governance. Both the UK Law Commission and the European Commission have produced extensive consultation papers and expert group reports addressing liability in digital environments, including mass hacking events and AI-driven systems [15; 18].

Importantly, the UK and EU frameworks offer transferable models for other sectors, including maritime operations. The legal dilemmas they face—such as gaps in software liability, unclear recovery pathways for insurers, and the need for public compensation schemes—mirror those confronting the shipping industry as it adopts autonomous navigation and cyber-reliant systems [21; 22]. Thus, the UK and EU serve as both case studies and conceptual baselines for developing cross-sectoral governance approaches to cyber risk in automated transport systems.

4 RESULTS AND DISCUSSION

4.1 *The Challenge of Attributing Liability in Mass Hacking Scenarios*

The attribution of liability in the aftermath of a mass hacking event involving autonomous systems presents a complex legal and policy challenge. Unlike conventional accidents caused by mechanical failure or human error, cybersecurity breaches often involve intentional third-party interference, sophisticated techniques to mask origin, and impacts across multiple users or systems simultaneously. These characteristics complicate fault determination and the subsequent allocation of responsibility among manufacturers, software developers, fleet operators, insurers, and end users [4; 8; 26].

Product liability frameworks offer limited relief in such scenarios. Under the UK's Consumer Protection Act 1987, claimants must demonstrate that a product was defective and that the defect caused damage. However, cybersecurity vulnerabilities may not manifest as traditional defects. Rather, they often emerge as latent risks, only exposed through exploitation by malicious actors [26; 34]. In some cases, manufacturers may invoke the "state-of-the-art" defence, arguing that the risk could not have been known at the time of production [17; 18]. This limits liability and restricts insurers' ability to recover compensation through subrogation, particularly when updates were issued post-manufacture but prior to exploitation.

Even when attribution to a software component is possible, the fragmented nature of modern vehicle production complicates recourse. Different entities may be responsible for various hardware, firmware, and data management systems. As observed in maritime regulation, similar attribution issues arise in the context of unmanned ships, where fault may involve system designers, onboard software providers, or third-party communication services [21; 22].

Another challenge lies in the evidentiary burden required to trace the source of a cyberattack. The sophisticated nature of hacking methods, often leveraging obfuscation or distributed attack architectures, can delay identification of the breach point. This delay can undermine legal proceedings and increase the likelihood of victims being left without redress, particularly where no-fault insurance or public compensation mechanisms are absent [20; 23].

Furthermore, mass hacking incidents create systemic risk: when identical vulnerabilities are exploited across a fleet or system, the aggregated damage may be substantial, exceeding the capacity of individual insurers or contractual frameworks. This has led to concerns over the insurability of such events, with some insurers already expressing reluctance to provide cover for catastrophic cyber risks in the transport sector [35]. In these instances, the absence of a central guarantee fund or reinsurance pool increases exposure for users and third-party victims.

Addressing these attribution challenges will require not only technical improvements in system traceability and cyber resilience but also legal and institutional reform. Liability regimes must evolve to reflect the distributed and invisible nature of cyber harm, with clearer standards for causation, evidence collection, and fault apportionment. Without such adaptations, victims in maritime autonomous systems may remain vulnerable to legal uncertainty and uncompensated loss.

4.2 *Role of Insurers and the Limitations of Current Coverage*

Insurers play a pivotal role in mitigating the risks associated with cybersecurity breaches in autonomous systems, yet current insurance frameworks remain ill-equipped to manage the scale and complexity of cyber-induced losses. In traditional transport contexts, insurance mechanisms are structured around identifiable fault and foreseeable loss. However, cyberattacks disrupt these foundations by introducing anonymity, system-wide impacts, and interdependencies between hardware, software, and infrastructure actors [8; 23].

The AEVA attempts to address these challenges by imposing a first-party liability model in which insurers

compensate victims directly for harm caused while a vehicle is operating in automated mode [12]. This approach enhances certainty and access to compensation but places insurers at the frontline of cyber-risk exposure without offering clear avenues for recouping losses from manufacturers or software suppliers. The difficulty in proving software defectiveness or negligence following a cyberattack—especially in real-time, over-the-air systems—creates barriers to indemnity claims under product liability law [14; 18].

Exacerbating these challenges is the potential for mass-risk events, where identical vulnerabilities in software systems lead to simultaneous failures across multiple vehicles or systems. Such events may trigger aggregated losses that exceed insurers' solvency thresholds or reinsurance capacity. In these scenarios, the reluctance of underwriters to provide full cyber coverage has become increasingly apparent. Some insurers are excluding cyber-related incidents from standard policies or capping coverage to limit exposure, which undermines the protective intent of AEVA and similar regimes [35].

These limitations are not unique to road transport. Maritime insurers face analogous challenges, particularly as unmanned ships and cyber-reliant port systems grow in complexity. Traditional marine insurance often excludes losses caused by "war, strikes, and malicious acts," which may include state-sponsored or anonymous cyberattacks [21; 22]. Without sector-specific reforms or shared-risk mechanisms, such as reinsurance pools or guarantee funds, insurers may be unable or unwilling to underwrite catastrophic cyber liabilities.

4.3 *Manufacturer Responsibilities and Potential Legal Defences*

Manufacturers of CAVs occupy a central position in cybersecurity governance due to their control over embedded software, hardware configurations, and system integration. In theory, this control creates a strong case for liability when cybersecurity breaches result in harm. However, existing legal frameworks offer manufacturers several defences that may limit or exclude their responsibility, complicating recovery for victims and insurers alike.

Under product liability law, including the UK's Consumer Protection Act 1987, manufacturers can be held liable for defects that render a product unsafe [14]. Yet in the context of software-driven vehicles, proving defectiveness is complex. Cyber vulnerabilities may result from unforeseeable interactions between systems or from evolving threats not known at the time of development. As a result, manufacturers may invoke the "development risk" defence—also known as the "state-of-the-art" defence—arguing that the risk could not have been detected using existing knowledge and technology at the time of production [17; 18].

Additionally, manufacturers may avoid liability where users have failed to install software updates that address known vulnerabilities. The AEVA 2018 allows insurers to exclude liability or seek reimbursement if the vehicle owner neglects to install safety-critical updates [12]. However, this raises concerns about the fairness and feasibility of expecting non-specialist users to manage complex cybersecurity requirements, especially in real-time operational contexts [30].

These issues are echoed in maritime systems, where shipbuilders and technology suppliers similarly resist broad liability for cyber-induced losses. In both sectors, the diffuse nature of technological responsibility—spread across component suppliers, software developers, and integrators—undermines clear accountability. Without regulatory mandates clarifying minimum security standards and liability triggers, manufacturers may continue to evade responsibility through legal ambiguity and contractual disclaimers [22; 18].

Effective governance will require legal frameworks that balance innovation with accountability, ensuring that manufacturers cannot avoid liability through structural or evidentiary gaps. Clear statutory definitions, coordinated cyber standards, and equitable burden-sharing between users, insurers, and producers are essential to protect stakeholders in autonomous transport systems.

4.4 *The Need for a National Compensatory Mechanism*

Given the limitations of existing insurance and liability frameworks in addressing the consequences of mass cybersecurity breaches involving autonomous systems, a strong policy case emerges for the establishment of a national compensatory mechanism. Such a mechanism would ensure that victims of cyber-induced harm are not left uncompensated due to legal uncertainty, insurer exclusions, or challenges in attributing fault.

The MIB currently serves this function for uninsured or untraced drivers under the Road Traffic Act 1988, offering a precedent for a publicly supported fund designed to cover compensation gaps [9; 11]. However, the MIB model is not designed to address the complexities of systemic risk or digital causation. In scenarios involving coordinated cyberattacks on fleets of autonomous vehicles or vessels, the scale and anonymity of the event may overwhelm conventional insurance and tort mechanisms [8; 23].

One solution proposed in the literature is the establishment of a reinsurance pool or publicly administered fund, akin to the UK's Flood Re scheme, which enables insurers to transfer catastrophic risk into a collective model supported by public-private cooperation [4; 23]. This model could be extended to cover losses stemming from cyberattacks on connected and autonomous systems, including those in maritime and port infrastructure where similar risk profiles exist [21; 22].

A national compensatory mechanism would also reduce litigation costs and delays by decoupling victim compensation from the complex task of fault attribution. It could operate under a strict liability standard, providing predictable outcomes for victims while allowing insurers and manufacturers to resolve contribution disputes separately. This approach would align with broader public interest goals, including safety, resilience, and the promotion of technological innovation without disproportionate liability exposure.

Implementing such a mechanism requires careful legislative design, including clear criteria for triggering compensation, funding models, and integration with existing insurance and regulatory structures.

To operationalize the proposed national compensatory mechanism, it is essential to outline its funding model. A logical source would be a modest levy on existing insurance premiums for users of connected and autonomous vehicle (CAV) systems and maritime transport operators. Drawing on analogies from the UK's Flood Re scheme and the Motor Insurers' Bureau (MIB) model, it is estimated that a surcharge of approximately 2–5% on standard premiums could sustainably finance such a fund without imposing prohibitive costs on users. This approach would spread the risk equitably across the sector, reflecting the collective interest in maintaining public confidence and systemic resilience against mass cyberattack events. Precise actuarial assessments would, of course, be needed to calibrate contribution rates accurately based on sector-specific risk profiles and loss modeling.

As autonomous transport systems evolve, this proposal offers a proactive solution to bridge the growing gap between technological complexity and legal protection.

4.5 *Policy Implications for Other Autonomous Transport Sectors*

The legal and insurance challenges associated with cybersecurity in CAVs have broader implications for other high-risk, automation-driven transport sectors—most notably maritime and aviation. These sectors are similarly undergoing digital transitions, relying increasingly on software-driven systems, remote connectivity, and artificial intelligence for core operational functions. As such, they are exposed to the same structural vulnerabilities and legal uncertainties already evident in the CAV domain.

In maritime transport, the rise of unmanned vessels, autonomous navigation systems, and smart port infrastructure raises new questions about liability allocation when cyber breaches cause physical or financial harm [21; 22]. Traditional maritime law is premised on human oversight and fault-based attribution. As cyber-physical systems replace crewed operations, existing liability regimes may fail to account for damages arising from AI error, system malfunction, or undetected cyber intrusions. The absence of mandatory cyber standards and enforceable accountability mechanisms mirrors the legal fragmentation seen in the CAV context [18].

Aviation systems, though subject to stricter international regulation, also face governance gaps in managing risks related to autonomous drones, remote piloting, and AI-based air traffic control. As with CAVs, liability in aviation may be obscured by the layered responsibilities of system designers, software vendors, and operators, especially when attacks exploit vulnerabilities unknown at the time of deployment [8; 26].

Policy responses across these sectors can benefit from a shared conceptual and regulatory foundation. Lessons from AEVA 2018, the MIB, and proposed national compensation models may serve as transferable frameworks for managing cyber-risk, especially in cases of mass disruption or attribution difficulty [4; 23]. Coordination between regulators, insurers, and manufacturers across sectors is essential to develop interoperable standards and cohesive liability structures.

Ultimately, as automation becomes a common feature of global transport systems, cross-sector policy learning and harmonized legal adaptation will be crucial to ensuring that cybersecurity incidents do not undermine trust, safety, or innovation.

These findings offer several practical implications for regulatory bodies, insurers, technology developers, and transport operators. First, policymakers can leverage the proposed national compensatory mechanism to bridge current liability gaps, ensuring that victims of cyber-induced incidents are compensated without undue delay or litigation. Second, insurers are encouraged to reassess policy wording and risk pooling strategies to better accommodate systemic cyber risks associated with autonomous systems. Third, manufacturers and software developers should integrate cybersecurity standards more deeply into product design and maintenance protocols, reducing vulnerabilities that lead to mass-risk events. Finally, in the maritime sector, stakeholders can apply similar compensatory and liability-sharing models to mitigate cyber risks in autonomous shipping and port operations, ensuring sectoral resilience in the face of growing technological interdependence.

5 CONCLUSIONS

The increasing integration of autonomous technologies into transport systems has introduced significant cybersecurity risks that challenge existing legal and insurance frameworks. Connected and autonomous vehicles (CAVs) exemplify the difficulty of applying traditional fault-based models to cyber-physical incidents, particularly those involving intentional third-party hacking or latent software vulnerabilities. These incidents often defy easy attribution and create legal uncertainty, exposing victims to potential gaps in compensation and insurers to unquantified systemic risk.

This paper has demonstrated that while legislative efforts such as the UK's Automated and Electric Vehicles Act 2018 (AEVA) represent meaningful progress, they remain insufficient in addressing the complexity of cybersecurity-induced harm. Key gaps persist in the areas of software liability, insurer recovery rights, and manufacturer accountability. The existing reliance on product liability and user compliance with software updates is inadequate when mass-risk scenarios or unknown vulnerabilities are involved.

The role of insurers is similarly constrained by coverage limitations and an absence of viable mechanisms for managing large-scale cyber loss. As the threat of catastrophic cyber events grows, particularly through coordinated attacks on fleets or infrastructure, the insurability of autonomous systems comes into question. This concern is equally present in

maritime and aviation sectors, where digital transformation is accelerating without equivalent legal modernization.

In response, this paper advocates for the creation of a national compensatory mechanism to ensure equitable and reliable redress for victims of cyber-related transport incidents. Drawing from the Motor Insurers' Bureau and Flood Re models, such a mechanism would allow for collective risk pooling, alleviate burdens on insurers, and provide legal certainty in complex or anonymized attack scenarios.

Beyond CAVs, the policy lessons identified in this study carry broader relevance for autonomous maritime systems, where legal and institutional inertia may hinder the safe adoption of cyber-reliant operations. Cross-sectoral coordination, harmonized standards, and proactive regulatory reform will be essential to ensure that legal protections evolve in tandem with technological capability. Without such measures, the public trust and systemic resilience needed to support next-generation transport systems may remain at risk.

REFERENCES

[1] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898–2915, Nov. 2017, doi: 10.1109/tits.2017.2665968.

[2] C. Lee, "Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars," Federal Communications Law Journal, vol. 69, 2017.

[3] C. Kennedy, "New Threats to Vehicle Safety: How Cyber Security Policy Will Shape the Future of Autonomous Vehicles," Michigan Telecom and Technology Law Review, vol. 23, no. 2, pp. 343–360, 2017.

[4] M. Channon, L. McCormick, and K. Noussia, The Law and Autonomous Vehicles. Informa Law from Routledge, 2019. doi: 10.4324/9781315268187.

[5] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk Assessment for Cooperative Automated Driving," Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy, pp. 47–58, Oct. 2016, doi: 10.1145/2994487.2994499.

[6] C. Ducuing, "Towards an Obligation to Secure Connected and Automated Vehicles 'by Design'?," Security and Law, pp. 183–214, Oct. 2019, doi: 10.1017/9781780688909.008.

[7] B. Walker-Smith, "Automated Driving and Product Liability," Michigan State Law Review, vol. 1, 2017.

[8] Z. Winkelman, M. Buenaventura, J. Anderson, N. Beyene, P. Katkar, and G. Baumann, "When Autonomous Vehicles Are Hacked, Who Is Liable?," 2019, doi: 10.7249/rr2654.

[9] Motor Insurers' Bureau, "Uninsured Drivers' Agreement," 2015.

[10] UK Parliament, Road Traffic Act 1988.

[11] MIB, "Articles of Association," 2019.

[12] UK Parliament, Automated and Electric Vehicles Act 2018.

[13] UK House of Commons, Public Bill Committee Debates on AEVA 2018.

[14] D. Rowland, "Liability for Defective Software," Cambrian Law Review, vol. 22, pp. 78, 1991.

[15] UK and Scottish Law Commissions, "Automated Vehicles: Summary of Responses to Consultation Paper 3," 2021.

[16] S. Saxby, Encyclopaedia of Information Technology Law, Sweet & Maxwell.

[17] Society of Motor Manufacturers and Traders, "Connected and Autonomous Vehicles: Position Paper," Feb. 2017.

[18] European Commission, "Liability for Artificial Intelligence and Other Emerging Digital Technologies," 2019.

[19] J. Marson, M. White, and K. Ferris, "The Investigatory Powers Act 2016 and Connected Vehicles: A New Form of Panspectric Veillance Looming?," Statute Law Review, vol. 44, no. 1, Apr. 2022, doi: 10.1093/slr/hmac004.

[20] M. Channon, "Automated and Electric Vehicles Act: An Evaluation in Light of Proactive Law and Regulatory Disconnect," European Journal of Law and Technology, vol. 10, no. 2, 2019.

[21] F. Wang, "The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships," Journal of Business Law, no. 4, pp. 311, 2020.

[22] R. Veal and H. Ringbom, "Unmanned Ships and the International Regulatory Framework," Journal of International Maritime Law, vol. 23, no. 2, pp. 100–113, 2017.

[23] M. Schellekens, "No-fault compensation schemes for self-driving vehicles," Law, Innovation and Technology, vol. 10, no. 2, pp. 314–333, Jul. 2018, doi: 10.1080/17579961.2018.1527477.

[24] M. Schellekens, "Car hacking: Navigating the regulatory landscape," Computer Law & Security Review, vol. 32, no. 2, pp. 307–315, Apr. 2016, doi: 10.1016/j.clsr.2015.12.019.

[25] UN Task Force on Cyber Security and Over-the-Air Issues, "Draft Recommendation," UNECE WP.29 GRVA, 2018. [Online]. Available: https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf

[26] European Parliamentary Research Service, "A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles," 2018.

[27] Centre for Connected and Autonomous Vehicles, "Key Principles of Vehicle Cyber Security for Connected and Autonomous Vehicles," 2017. [Online]. Available: https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[28] J. Prior, "Connected and Autonomous Vehicles, Cyber Threats and the UK Motor Insurance Framework," Exeter Law Review, vol. 46, pp. 126, 2021.

[29] Centre for Connected and Autonomous Vehicles, "Safe Use of Automated Lane Keeping System (ALKS): Call for Evidence," Aug. 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/911016/safe-use-of-automated-lane-keeping-system-alks-call-for-evidence.pdf

[30] Venturer Project, "Driverless Cars: Liability Frameworks and Safety by Design," Insurance and Legal Report, 2018. [Online]. Available: https://www.venturer-cars.com/wp-content/uploads/2018/06/Year-3-Legal-and-Insurance-Report.pdf

[31] Hardy v Motor Insurers' Bureau [1964] 2 QB 745.

[32] Bristol Alliance Ltd v Williams [2012] EWCA Civ 1267.

[33] European Parliament and Council, "Regulation (EU) 2019/2144 on the Type-Approval Requirements for Motor Vehicles," 2019.

[34] M. Jones, A. Dugdale, and M. Simpson, Clerk and Lindsell on Torts, 22nd ed., Sweet & Maxwell, 2017.

[35] Department for Transport, "Pathway to Driverless Cars: Government Response," 2017.