

Jean Monnet Module
SCHOOL OF ADVANCED SOCIAL STUDIES

Sustain4EU: Enhancing European Civic Practices and Sustainability as the articles for this thematic issue were collected within this project.



With the support of the Erasmus+ Programme of the European Union

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Open Access. © 2023. Ramnath Reghunadhan. This is an open access article distributed under the Creative Commons Attribution-NonCommercial-NoDerivs license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Original Scientific Article • DOI: 10.2478/rsc-2023-0004 • RSC • 15(1) • 2023 • 40-52

Research in Social Change

AUTONOMOUS VEHICLES AND THE LINKAGES TO SMART MOBILITY: IMPACT AND IMPLICATIONS ON DIGITAL GLOBALISATION

Ramnath Reghunadhan[1,*], Ansel Elias Stanley[2]

[1]*Assistant Professor of Politics, Department of International Studies, Political Science and History, Christ (Deemed to be University), Bengaluru, India*
[2]*Doctoral Candidate, Centre for East Asian Studies, School of International Studies, Jawaharlal Nehru University, New Delhi, India*

Abstract

Human civilisation is undergoing a transformation, perceived as the institutionalisation of digital globalisation. The 20th century witnessed greater strides in the form of the internet revolution, automobile technologies and smart mobility, related transformation, dissemination and integration of related technologies as well, leading to the emergence of digital globalisation. The integration of cyber-physical systems has accelerated the rate of urbanisation, and the currently prevailing enhanced standards of living have increased the number of automobiles in cities that have been integrated into the digitally globalised ecosystems, leading to the emergence of autonomous vehicles (AVs). The present study analyses the emerging threats and vulnerabilities of AVs and smart mobility, which have created more security concerns for AVs across nation-states, leading as well to the emergence of digital globalisation. The article theorises the aspects of human security linkages and utilises a capacity matrix (qualitative approach) to examine the development, institutionalisation and integration of AVs into digital globalisation and the related challenges emerging along with it.

Keywords

autonomous vehicles • digital globalisation • human security • cybersecurity • smart mobility

1. Introduction

The 21st century will see increased population mobility, (potentially) resulting in a much greater need to integrate, encompass, incorporate and connect netizens to the (digital and cyber) systems and services within societies. Human security is interconnected through digital (urban) ecosystems to provide for these changes and drive people into the next era of efficiency. This has a multiplier effect on human security linkages in societies – taking into account the socioeconomic, political and psychological natures of human beings. Every relation, information, thought process, act of decision-making and life has been digitised here. Being touted as Urbanization 2.0, an interesting aspect of this digital globalisation is that it will perpetuate into every facet of human security, and particularly, connectivity, transportation and related infrastructure are no exceptions to it. Today, more than half the world's population lives in urban areas, and this figure is expected to increase to more than 65% within the next three decades (UN 2014; Bildt 2017; Reghunadhan 2018b; 2019). This points to the fact that the growth engine of the world and the greatest impact of population growth and migration will have a profound impact on the world's urban areas.

The issues of sustainability and governance challenges will readily impact most of the urban areas around the globe. It is estimated that, by 2050, there will be an increase in the total population in these urban areas by more than 2 billion. The technology is usually associated with smart cars, but it also encompasses a set of other vehicles such as trucks, buses and unmanned aerial vehicles (UAVs). The application of this technology is not limited to the transportation sector but encompasses also the agriculture, industry, service and military sectors. These would be interconnected and controlled through smartphones, Wi-Fi features and other related technologies that would provide greater user interface and usability (Kato et al. 2015, 60–8; Reghunadhan 2022). A self-driving car is even linked to climate change, environmental sustainability, emission-free smart cities and mobility across countries (Balasubramanian 2015), which entail imbibing emergent (digital) technologies to accelerate the process of connectivity, infrastructural and economic development. Bilateral and multilateral cooperation between various countries has elucidated the need to include autonomous vehicles (AVs) as a major imperative. The study attempts to elucidate the following research questions:

Corresponding author e-mail: vrramnath@gmail.com;ramnath.reghunadhan@christuniversity.in

© 2023 Reghunadhan and Stanley, This is an open access article distributed under the Creative Commons Attribution-NonCommercial-NoDerivs license (https://creativecommons.org/licenses/by/4.0/).

(a) What are the transformations and ramifications of AVs and smart mobility for digital globalisation? (b) What are the human security needs, vulnerabilities and capacity matrix for AVs in digitally globalised ecosystems? (c) What are the future practical suggestions and opportunities for growth of AV (eco) systems for digital globalisation?

2. Research Methodology

The present study utilises a qualitative approach, entailing case studies, content analysis and textual analysis. It undertakes an in-depth analysis of various facets and aspects of smart mobility and AVs, contextualising and theorising the developments and transformations in society. It critically examines the AV systems through a human security approach, bringing in various parameters and characterisations. Content analysis of various reports, agencies and organisations was also undertaken to provide analytical reports intended to bring out the inherent issues of AVs and provide a narrative to theorise the human security approach. Accordingly, the emergence of digital globalisation is linked to developments in smart mobility and is intricately linked to AVs. The study utilises the human security approach (UNDP 1994) in order to analyse various facets related to AVs and the linkages to smart mobility, as has been explained in the following section.

3. Smart Mobility

The concept of AVs and smart mobility is at the centre of the future, and has emerged and is seen as an exponential rise in the 21st century. The global AV market was valued at 54.23 billion USD in 2019 and is projected to grow to 556.67 billion USD by 2026 (AMR 2018). During recent times, AVs are expected to generate 'more employment and enhance the ease of living' in relation to transportation and connectivity (PIB 2018; 2021a; 2021b). Incidentally, *smart mobility and transportation* have been identified as amongst the 'five fields to focus on implementing' artificial intelligence (AI) (Hebbar 2018, Reghunadhan 2022: 85). However, a major concern and challenge in this regard will thus be to streamline and provide equitable access to the new digital technologies that include the need for smart mobility through *smart transportation*, one which can revolutionise 'how cities operate and are organized' (Ding et al. 2015). This is evident in the emergence of technologies tested and used in AVs, which are expected to rise exponentially. AVs can be defined as '*a vehicle that is capable of sensing its environment, interpreting information coming from a variety of sensors embedded in the vehicle and safely performing necessary functions of the vehicle with a little or no human intervention*'. The concept of smart mobility is gaining momentum around the world, with emerging markets across North America, Europe, Asia and Australia (Redican and Zhang 2020; PIB 2021a; 2021b). Owing to the perceived benefits of smart mobility, the necessary infrastructure is rapidly being built to support this endeavour through a large deployment of the AVs. The future of AVs and smart mobility, pertaining to the rise and integration of the Fourth Industrial Revolution and smart cities, is right around the corner.

In 2012, an addendum in the form of a new field called deep learning emerged, providing greater accuracy in speech and image recognition, transforming manufacturing, production mechanisms and provision of services for smart cars. They can influence decision-making in the interconnected internet of things (IoT) devices and manipulate big data-linked services and many others. Elon Musk, the CEO of Tesla and Space X, has cautioned against the development and use of AI in AVs (Reghunadhan 2022). The potential dangers of using 'AI Doomsday' even revealed AVs laying the foundation of future conflicts between nations and as a future weapon of cyber hacking. Cyber threats would consequentially create greater ramifications when there would be a possible integration of biological and machine intelligence. The future of smart cars will transform as a human–machine interface and/or what is known as brain–computer interface (BCI), as well as interlinkages that have already been set up for enhancing cognitive capabilities under what is envisioned as 'neurotechnology' in different parts of the world. This has already been in the research loop at Musk's company, named Neuralink, and other major companies such as Facebook (in 2015) and Kernel (in 2016), entailing these integrations into AVs. This would create vulnerabilities to human security, particularly to the shaping and moulding of thought processes and ideas, as well as the susceptibility to cyberattacks from state or non-state actors and other similar entities (Reghunadhan 2018a).

The important examples are related to the developments in China and the European Union (EU). In China, Daimler became the first international automaker to be granted a licence to test self-driving vehicles on public roads, followed by Mercedes-Benz. The test vehicles' technical applications are said to be provided by Baidu, a prominent China-based multinational company linked to the development of emergent (frontier) technologies used in AVs. Baidu has developed the open-source autonomous driving platform, the Apollo programme, and partnered with over 100 domestic and foreign companies. Baidu is currently on track to massively produce 'autonomous mini-buses' and has started its services in Beijing, Shenzhen, Pingtan and Wuhan; meanwhile, autonomous 'buses will initially be deployed in tourist spots, airports and other controlled or geo-fenced areas' (Korosec 2018a; 2018b). Baidu's latest autonomous driving platform, Apollo 3.0, provides new and innovative solutions and supports

'valet parking, autonomous mini-buses and autonomous microcars' (*ibid*.). Similarly, the EU spent 787 billion USD during 2007–2016 under the Seventh Framework Programme (FP7), and the Horizon 2020 programme was initiated by the EU with a proposed funding of 94 billion USD over 7 years during 2014–2020, with an emphasis on innovation, capacity and skill building, as well as technological developments that focussed on lab-to-field (L2F) for AVs (EC 2019; 2020; 2022). In 2016, the European Defence Research Programme (EDRP) was initiated with requests for 582 million USD for research and development (R&D) for the period 2021–2027. The projects include European Technology for Unmanned Heterogeneous Swarm of Sensor Platforms for Defence Applications (EuroSWARM), Standardization of Remotely Piloted Aircraft System (RPAS), Detect and Avoid or Traffic Awareness Project (TRAWA) and Inside Building Awareness and Navigation for Urban Warfare (SPIDER) (GAC n.d.; EDA 2016; 2018; Boulanin and Verbruggen 2017, 103–4). The application of AV in the defence sector, particularly with weaponry development, has already been in the debate among experts, be it human security, privacy or national security ramifications inherent in the matter. AVs have been in development for different countries (but at varying levels), but with AI, there are huge ramifications (Stirling, Miller, and Martinho-Truswell 2018).

With the emergence of digital globalisation, emerging threats from denial-of-service (DoS) attack, distributed denial-of-service (DDoS) and other related botnet attacks, spoofing or middle-man attacks, insider exploitation and air-gapping have created more security concerns in AVs. The threats from different actors from cyberspace and other actors (including both state and non-state) could take control of AVs in a nation, and in turn, this could result in the unfolding of a sequence of events wherein the host nation is attacked and (possibly) even destroyed. Unlike the earlier conventional conflicts, the enemy need not even enter the territory of a nation but could (if not completely) destroy a nation and cause a magnitude of casualties using its (digitally connected) technological weapons against it. There could be a transformation of the very nature of conflict in the 21st century, where the transnational nature of cyberspace will create new complexities and intricacies in the emerging conflicts. The emergence of AI has created serious concerns about the inherent issues in the development, use and application of AVs, possibly creating more complex threats.

In the next decade, one-fourth of total cars are estimated to be self-driving cars, which can resolve the issues related to (traffic) congestion in major cities in Asia, especially in India. It is estimated that searching for a parking space mainly causes about one-third of the traffic congestion. Among all Asian countries, the traffic congestion is estimated to be the highest in India, averaging a whopping 149% (AMR 2018). According to the Boston Consulting Group's (BCG's) report, titled *Unlocking Cities: The impact of ridesharing across India*, the avoidable social cost of congestion due to traffic across major cities is 9.6 billion USD in Delhi, 5.92 billion USD in Bangalore, 4.8 billion USD in Mumbai and 1.97 billion USD in Kolkata (Tomtom 2020). According to a study conducted by Ford Motor Company, titled *Ford Driving Habits Survey*, 6 out of 10 instances of traffic congestion in India are reportedly caused by drivers. This could be easily eliminated by using smart technology and IoT, reducing the time spent for driving and parking, which means that individual users can alternatively use this same time for other, more productive purposes (Rolison et al. 2018).

On an annual basis, around 1.3 million people are killed in traffic accidents, mostly caused by human-induced error. These include issues caused by physical and emotional factors such as 'stress, fatigue, recklessness and there are also the instances of non-adherence to traffic rules, distracted driving by rampant use of mobile phones while driving, taking selfies, browsing social media and many others' (*ibid*.). R&D spending across the globe for developing technologies and digitalisation of AVs along with smart mobility will reduce (potential instances of) collisions through real-time communication and positioning of vehicles and reduce traffic congestion for both autonomous and semi-AVs. According to estimates, this could extricate billions of hours wasted on traffic jams annually. An estimated one trillion USD could be saved on fuel costs, and approximately 220 MMT of greenhouse gases (GHGs) can be prevented from entering the atmosphere. This will increase the air quality, reduce the incidence of diseases in urban and rural areas and help countries achieve sustainable development goals (SDGs) in an accelerated manner (*ibid*.; Reghunadhan 2019).

The implications for AVs and IoT comprise a wide range of factors in an ecosystem of interconnected and interrelated devices and services. It also includes sensors, smart consumer goods and industry and health sector components. Thus is facilitated the ability to gather, exchange, trade and/or even process any quantity of data in enabling adaptation to any particular context, as well as the capability for transforming businesses and even the 'way of living'. It is closely connected to cyber-physical systems concerning emerging and potential (future) safety implications. Some researchers have exposed the vulnerability of AVs of the company Jeep using zero-day exploits, which forced the recalling of around 14 lakh vehicles (Batty 2013).

Hackers (both *whitehat* and *blackhat*) and governments have identified the increasing vulnerabilities of vehicles of Tesla, Volkswagen and BMW (*ibid*.). The emergence of 'smart cars as systems providing connected, added-value features to enhance car users' experience or improve car safety … encompasses use [of] telematics, connected infotainment

or intra-vehicular communication.' However, cyber threats to AVs and IoT pose inherently greater challenges; safety and security will have to be addressed in the coming years (Parkinson et al. 2017; Yağdereli et al. 2015, 369–81; Reghunadhan 2018a). Dr Haim Wismonsky, the author of the book *Criminal Investigation in Cyberspace (2016),* opined that smart cars usually contain:

> In the past decades, vehicles are becoming more and more "smart". They contain more software, communication devices, and computer-based hardware than ever before, often connected to a wired and even wireless network. These vehicles are based on the CAN Bus (Controller Area Network) - a network that connects the electronic components of the vehicle and is largely responsible for its operation - from the use of electric windows to the use of vehicle brakes (Wismonsky & Shany 2016).

The 'intelligent public transport (IPT) systems' will be a key component of the smart cities and will manage the local public transportation system by applying digital technologies to improve efficiency and integrated service levels in the transport system. This will lead to a greater degree of automation[1] and interconnectedness in a city and create vulnerabilities and newer threat perceptions about 'data exchanges, privacy as well as the health and safety of citizens … [the lack of] harmonized guideline[s] or standard[s] to model these data exchange' (Lee, Kim, and Seo 2019).

The adoption of 'solutions with low scalability and disparate requirements' enables hackers to easily hack into the devices and communication networks, even crippling the physical infrastructure. IPT could become easily targeted and possibly hacked due to the inherently unreliable or obsolete security measures and mechanisms in place, possibly creating an impact on the economy, as well as the safety and health of citizens. With the steady compression of technology adoption cycles seen worldwide, innovations in this sector are expected to be accelerated (*ibid*.; White and Garry 2010). Any citizen or organisation with AVs, deployed whether in commercial or private use, will be interconnected to the digital globalisation technology that is emerging as part of the new era of digital urbanisation taking place around the world. However, all of this has serious ramifications and vulnerabilities that will also pose a greater risk to the users. This connected society brings challenges that have not been experienced before, such as cyberattacks and breaches of data privacy, or exacerbate some of the existing challenges such as economic disparity and food security in the world. The following section explores the ramifications of AVs and smart mobility through the human security approach.

4. Human Security Approach: Theoretical Underpinnings

In the early '90s, in the aftermath of the fragmentation of the Soviet Union, there was a global trend towards various models of security. This was seen in international institutions, especially the United Nations (UN). In 1994, the UN published and brought forth the Human Development Report, titled '*New Dimensions of Human Security*', which greatly emphasised the human security approach amongst policy makers, academia and civil societies (UNDP 1994). Since then, the developmental aspect of the nation-states was appended with the human security approach and soon became a mainstream framework in understanding (non-)state actions, activities, strategies and policies worldwide. This provided a variegated understanding of dealing with multiple threats and vulnerabilities within a nation, which traditional theorists, scholarly literature and policymakers have often discarded. Within international relations and politics, the human security approach has become the mainstay of analysing the performance of a nation-state and the indicator of scrutinising the security within and the implications (Broadhurst and Grabosky 2005; Bates et al. 2019).

The Human Development Report 2000, titled '*Human Rights and Human Development*', and Human Development Report 2001, titled '*Making New Technologies Work for Human Development*', characterise the aspects of digital, *communications and information technology*. They emphasised how '[c]yber networks have brought attention to rights, disseminating information on good practices and rights violations'. Thus, '[d]ata can be recorded, collated and publicly posted far more quickly and widely'. The emergence of the internet and other (means of) telecommunication systems have all reduced the cost and improved the means of communications (UNDP 2000: 39–120; UNDP 2001: 24–35). The Human Development Report 2009, *Overcoming barriers: Human mobility and development*, entails using digital technologies in smart mobility (UNDP 2009a). Figure 1 shows the different types of human security parameters (HSPs), including those of 'community security, economic security, environmental security, food security, health security, personal security, and political security' (UNDP 2009b).

The Human Development Report 2019, titled '*Beyond income, beyond averages, beyond today: Inequalities in*

1 Automation levels are based on standards developed by the SAE International and Case IH Agriculture. "Level 0: No Automation; Level I: Limited Assistance with human control, Level II: Partial Automation with human intervention, Level III: Conditional Automation with human planning, Level IV: High Automation in limited spaces, and Level V: Supervision using AI/Full Automation" (Cited from Reghunadhan and Stanley 2022).

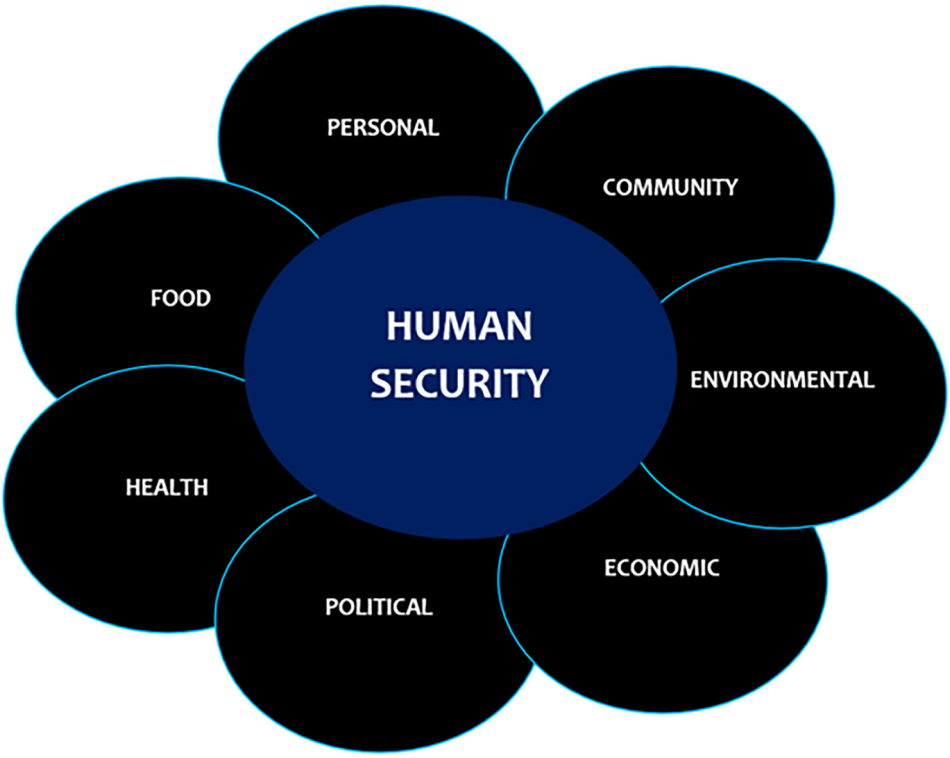


Figure 1. Types of human security approaches.
Source: Compiled by author from UNDP (2009b).

human development in the 21st century', focusses on the facets of *technological change* and the *reinstatement effect* in the digital age. The technological change entails 'automation, machine learning and robotics, new platform economy, global and local outsourcing', while the reinstatement effect entails 'cyber security experts, digital transformation specialists, data scientists' (UNDP 2019, 19–167). The Human Development Report 2020, titled '*The Next Frontier: Human Development and the Anthropocene*', entails the 'increasing economic value of digital goods and services (software, social networks, media, entertainment) … work, education, healthcare', with increasing connectivity facilitating the advancement of human security and development due to digital/cyber technologies. This was evident during the recent coronavirus disease of 2019 (COVID-19) pandemic, and the expansion of the digital sphere has transformed socioeconomic aspects across nations (UNDP 2020, 38–113; Reghunadhan and Stanley 2022). Table 1 undertakes a human security approach to analyse the pros and cons of AVs.

Here, P_{Co} is the HSP for community security, i.e. the impact on communities; P_{Ec} is the HSP for economic security, i.e. national (digital) economy; P_{En} is the HSP for environmental security, i.e. environment and/or climate change; P_{Fo} is the HSP for food/agriculture; P_{He} is the HSP for health security, i.e. healthcare sector and its implications; P_{Pe} is the HSP for individuals/citizens; and P_{Po} is the HSP for the political security, i.e. the political scenario in the state/country.

Based on Table 1, the implications of human security threats to digital globalisation have been demarcated into various parameters. These include community security, i.e. threats to communities, national and digital economy, impact on environmental security (including climate change), impact on food security (and agriculture in general), health security, personal security of citizens and political security within a state. This is evident in India, where integrating AVs could be part of the Provision of Urban Amenities to Rural Areas Initiative, including the PURA 3.0 Initiative. This will be a major lynchpin in order to semi- or quasi-digitalise rural areas in the country. The issues related to lack of direct access to services, a characteristic that can be observed particularly as one of marginalised communities (including poor and indigenous communities), are evidently related to the hierarchical issues of technology access and integration of AVs. Nevertheless, in terms of capacity building and accessibility, delivery of food, medicine and essentials to marginalised (ethnic) communities has been evident recently. The Director General of Civil Aviation (DGCA) has given the nod to companies for delivery of food and essential items in India utilising drones. This includes a consortium of drone start-ups such as 'Asteria Aerospace, Zomato, Swiggy and Dunzo' (Ray 2020;

Table 1. Human security needs, vulnerabilities and capacity matrix of AVs for digital globalisation

HSP	Needs/vulnerabilities	Capacities
P_{Co}	Lack of direct access to services and marginalisation from urban areas, suburbs and rural areas	Delivery of food, medicine and essentials to marginalised (ethnic) communities
P_{Ec}	Lack of access or technological connectivity, disparity and loss of jobs	Provision of fintech (including cryptocurrency), bank on wheels and digital economy
P_{En}	Complementing/supplementing technologies such as batteries increase pollution and e-waste.	Increases fuel efficiency, reduces pollution, streamlines processes and enables effective integration of renewables
P_{Fo}	Increase of cost in agroecosystems due to the deployment of high-end and frontier technologies	Increase in efficiency, accountability and transparency in interventions in agroecosystems
P_{He}	Data privacy issues, cyber threats to healthcare services and hacking of digital health	Data connectivity and real-time consultation, decision-making and provision of emergency services
P_{Pe}	Cyber threats due to data and cybersecurity-related vulnerabilities, issues of data privacy and identity theft	Improvements in standard of living, access to technology, increasing ease of storage of information, reduction of accidents and psychological impact from driving-related activities
P_{Po}	Implications of growth versus development, and threats to CNI	Optimisation of resource usage, creation of new jobs, soft power and national security enhancement

Source: Compiled by authors.
CNI, critical national infrastructure; HSP, human security parameter.

Reach Project 2020). This has a huge impact on the aspects related to community and food security.

The use of AVs for food distribution and health security was evident in the activities of companies, agencies and organisations that have provided and leveraged long-distance delivery using drones to deliver life-saving and critical medicines and other essentials such as blood, personal protective equipment (PPE) kits, medicines and vaccines to health facilities in countries across Africa and Asia. During floods, drones played a huge role in geospatial mapping, assessing the damage and providing rescue and relief operations (Diwaker 2018; ETHealthWorld 2019; Zipline 2021). Besides, companies such as DJI, Volocopter, DroneDeploy and Skycatch have also undertaken various activities related to smart air mobility (including taxis), drone mapping and analytics, autonomous capturing of 3D drone images, e-business, etc. Various agricultural start-ups such as Marut Drones, TartanSense, Raptor Maps and many more across the world are using UAVs and smart tractors for 'smart agriculture'-related activities such as spraying pesticides, herbicides and fertilisers, planting seeds and monitoring and identifying problems in crop fields using aerial images of fields (Reghunadhan 2019; Crunchbase 2021).

Autonomous trucks have been deployed by companies such as Daimler, Benz, Volvo, Ford, BMW, Baidu and Tencent; start-ups such as Tesla and Rivian are developing and deploying autonomous trucks and cars. This has, to a large extent, mitigated the issues regarding the lack of optimally skilled drivers, on-time delivery and inefficiency, and problems related to human security. The automation of the financial industry will be accelerated due to the deployment of AVs and thus transform with the emergence of digital globalisation across national economies. The car industry's traditional payment and financial services will be replaced by a newer 'digital-first approach' to cater to the need of the AV ecosystems. This ranges from payments for external services while using the vehicle or payments for in-car services while operating the vehicle (Brunette and Eshel 2020; Redican and Zhang 2020).

The World Health Organisation (WHO) estimates that more than 1.25 million people die annually in traffic accidents, with an estimated cost of 5% of gross domestic product (GDP) in middle- and low-income countries. In India, 17–18 people reportedly died every hour from road accidents (the highest) in 2019 (NCRB 2021). Smart cars could reduce, if not eliminate, these human-induced errors. AVs are connected, controlled and monitored by sensors and applications that provide a real-time alert and response systems under the prevalence of ever-changing and complex conditions. Since machine-based intervention, especially that involving AI, will ensure that human-induced errors are eradicated to an enormous extent, after the institution of automation, there has been a shift in responsibilities to those responsible for the production as well as to the manufacturers (Audenhove et al. 2014; Janai et al. 2020).

The automotive sector will have enhanced and perfected smart technologies; increased investment in R&D by manifolds will revolutionise smart mobility and transportation. This is particularly important in urban areas where space is always a scarce public good and costly to afford. Integrating AVs that are interconnected to the digitally globalised ecosystems is expected to streamline traffic movement in urban areas and reduce traffic accidents, particularly through extensive use of enhanced sensors and technological innovations (*ibid*.). The Uru-Eu-Wau-Wau tribes, with the support of non-governmental organisations (NGOs), are using drones in the Amazon forest (Brazil) to check deforestation and other illegal logging activities (Lang 2020).

Drones have been increasingly used for agriculture and allied activities, and agricultural drones are considered the future of farming. In terms of personal and health security, accidents and health-related damages are expected to be reduced by AVs. Traffic congestion, health and other related stress are very high and can be reduced with the introduction of AVs. The political and national security implications of large-scale DDoS attacks by hacking AVs are also a huge threat. In terms of smart mobility, it is estimated that it amounts to a huge number of CO_2 emissions and other pollutants from the transportation sector (Krishna 2018; Filho et al. 2020; Librán-Embid et al. 2020, 139204). The introduction of AVs, especially cars, trucks and buses, can provide a huge leeway in that regard. This can enhance smart mobility and reduce congestion, accidents and pollution. Thus, health hazards and the impact of climate change can be reduced on a large scale. Further, even though countries try to build regulatory frameworks and governance structures for AVs, these proposals have largely remained on paper. This is mainly because of bureaucratic redtapism, a lack of skill and understanding that continues to persist despite sporadic public outcry insisting on amelioration of the situation, and functions based on largely outdated structures and workflows as compared with their Western counterparts. This directly affects 'decision-making, risk-aversion, administrative' endeavours, accountability and policy implementation (Sneha et al. 2021). The explosion of data coupled with the emergence of Industrial Revolution 4.0 has undergone a digital revolution that is particularly dependent on data-driven computing capabilities and automation. This has created a multitude of dimensions for human security related activities, industrial goods and processes. However, the issues of monopolisation of data collection and storage by some have created larger challenges that could be interlinked with the Cambridge Analytica and Facebook issue. The emergence of a digitally globalised ecosystem has the new oil in the form of data, which is touted to be the biggest resource that state actors and companies are after. There are issues with data sovereignty, accessibility, privacy and manipulation. This has enabled the threat of the creation of an 'Orwellian State', similar to that in China, where citizens practically lack privacy and are subjected to what Foucault considers as a 'surveillance state' and the perpetuation of 'disciplinary power' over the population (Foucault 1977; Lyon 1993, 1994; Reghunadhan 2018b), via a 'new surveillance' approach (Marx 1988; 2003).

The development and widespread use of AI have created greater potencies for new and emerging threats. The emergence of open-source software reduced cost, and greater accessibility of cyber technology has created a greater likelihood of attacks from non-state actors as well. This has increased the incidences of attacks, be it spam mails, phishing, social engineering-related attacks, identity theft or the mammoth DDoS attacks through AVs. There should be greater understanding, awareness, training, coordination and skilling of various actors and users in dealing with cyberattacks. Unquestionably, these threats and challenges have created a greater need for countries to ensure greater cooperation and coordination among various state and non-state actors. A universal acceptance of multi-stakeholderism around the globe for ensuing the creation of a cybersecurity architecture in dealing with cyber threats has become a necessity.

5. Suggestions and Way Forward

The impact of AVs on digital globalisation that interlinks with human security is an increasing concern for state actors, non-state stakeholders and individual (non-)citizens. Thus, there is a need to improve security mechanisms and measures in AVs, which have been threatened due to vulnerabilities arising from hacking. The way forward is to increase resilience and (cyber)defence at attrition-level activities. The manufacturers and industrial players need to establish best practices related to standardisation, scalability and effective security enhancement for their (end- and intermediate-) users.

Presently, there is a dire need to regulate the proliferation of new digital technologies. The legal framework of any country, or even the world as a whole, has not been able to catch up as technology advances rapidly and swiftly. Technology is also linked to the national prowess of a country, and most countries involved have taken a 'wait-and-watch' policy, the intention being not to stifle innovation in the sector. The authors propose a consensus model based on international guidelines inclusive of all national, regional and global stakeholders that must be followed to regulate technology whenever possible. A consensus model based on guidelines will not only help states regulate AV and related technology but also bring about a standardisation of the technology framework and avoid conflict across the world.

Smart cars must improve security mechanisms and measures to increase resilience and defence at attrition activities. The manufacturers and industrial players need to establish resilient systems and good practices that can enhance their users' security. The information sharing and exchanges should also include inputs from security researchers and relevant third parties. This should focus on enhancing and increasing the number of contact points with various cyber security experts and legal practitioners to provide greater security and protection against any new attack. There should be increased information sharing between manufacturers, production units, industrial producers, institutional mechanisms, cyber security units and other related stakeholders. This could provide an updated front of cyber defence against any emerging complex targeted attacks on particular vulnerabilities of the products

as well as users. The field information provides a greater understanding of ground realities and enhances the resilience of smart cars and AVs.

Whenever any security issues arise, there should be a clear-cut insight into and definition of issues and processes of liability among various actors, be it the manufacturer or the user(s). Besides, there should also be a consensus benchmark as well as a documentation on the technicalities and standardisation of best practices and context for future reference. This will enable greater independence (relative autonomy), and quality management evolves with new complexities to deal with the emergence of digital globalisation. Regular auditing and evaluation of the existing safety standards for automotive systems should be in place. This reduces errors, prevents and even mitigates security vulnerabilities and loopholes and enhances confidence for further investment and branding. An independent evaluation scheme for checking and authenticating quality on an annual or biannual basis would be a necessary preventive measure against potential vulnerabilities that could emerge. However, strict adherence to the quality of the independent evaluation agencies and/or organisations should be maintained so that no compromises in quality or security happen. This could also provide tools for a better analysis of the security measures in place, provide greater skillsets to the company personnel (as a whole) and ensure greater control and efficiency.

To prevent issues connected with breaches in data integrity from arising, particularly through the misuse of information and communication technologies (ICTs) for malignant and/or anti-social activities, or to prevent their exacerbation in case they have already arisen, the requirement is felt for not only a greater coordination between different actors, state and non-state, but also a larger collaboration among netizens; in the same vein, the need to formulate strategies arises as a prerequisite, particularly with the objective of developing frameworks capable of enabling support for policies, activities and implementation tasks aimed at mitigating the impact from cyber threats and attacks. The legal and institutional support, particularly pertaining to the capacity building of multiple agencies, requires collaboration and cooperation between different actors. The role of government in this regard remains important, as it enables the development of proactive but relatively effective legislative mechanisms, procedures and processes to deal with the cyber threats and attacks. This has to be supplemented by ensuring information sharing and cooperation between institutional actors by providing requisite training, tools and skills to deal with the emergent threats from cyber threats and attacks.

The information sharing and exchanges should also include inputs from security researchers (whitehat hackers) and relevant third parties, i.e. contact points with various cyber security experts and legal practitioners. The protection of and respect for the individual's (data) privacy should take precedence, which balances the national security–individual privacy debate, a golden mean in that regard. There should be increased information sharing between various manufacturers, production units, industrial producers, institutional mechanisms, cyber security units and other related stakeholders. This could provide an updated front of cyber defence against any emerging complex targeted attacks on particular vulnerabilities of the products and users. The field information provides a greater understanding of ground realities and enhances the resilience of smart cars and AVs.

Regular testing, auditing and evaluation of the existing safety standards for AVs and related systems should be in place. This could also provide tools for better analysis of security measures in place, provide greater skill sets to the company personnel as a whole and ensure greater control and efficiency. The issues related to standardisation, benchmarking and scalability should be addressed in order to ensure the institutionalisation, use and integration of best practices and mechanisms in place.

There is a need to prevent any exacerbation of cybersecurity-related issues, particularly through the misuse of information and communication technologies (ICTs) for malignant and/or anti-social activities (Reghunadhan 2020a; 2020b). This has to be dealt with based on a greater coordination, interoperability and scalability between various systems. Also, the need to formulate strategies and mechanisms, particularly for developing frameworks capable of enabling support for policies, activities and implementation tasks aimed at mitigating the impact caused by cyberattacks, is a prerequisite. The legal and institutional support, particularly with regard to capacity building of multiple agencies, actually requires collaboration and cooperation between different actors in the development of AVs.

The role of the state in this regard remains important, as it enables the development of proactive but relatively effective legislative mechanisms, procedures and processes to deal with the threat of cyberattacks. This has to be supplemented by ensuring information sharing and cooperation between institutional actors that respect and protect data privacy, residency and sovereignty. This can be undertaken by providing requisite training, tools and skills with which to tackle the threats emerging from cyberattacks (Reghunadhan 2018a). The stakeholders must increasingly ensure equity in these systems, reduce incidences of discrimination and (social) bias and increase accessibility. Further, effective steps should be taken to bridge the gaps in internet connectivity, autonomous technology and educational activities. Additionally, steps to reduce structural and technological divides between the rural and urban centres are required to be implemented.

There should be programmes to uplift or remedy the workforce displaced by automation. They must also be maintained a fine balance in the regulation of automation to ensure that the least amount of people are affected by it. The implementation of various initiatives to enhance skill through educational institutions should be ensured. Students, researchers and the workforce, in general, should be effectively skilled to meet the requirements of a largely automated workplace. This ensures that the rapid adoption of AV technology does not blindside them. With this, the process of digitalisation, IoT and the need for smart mobility will enable greater integration of the AVs into the emerging digital globalisation. This will also provide an effective cyber governance architecture and regulatory mechanisms to deal with the emerging complexities and challenges. It could provide for achieving SDG targets under the SDG '*Good Health and Well-Being*', which emphasised reducing to half the total number of global deaths and related injuries from road traffic accidents by 2020. The use of smart technologies in the emerging digital society and the integration provide greater efficiency in decision-making and enable efficacious use of spaces.

6. Conclusion

The transformations and ramification of AVs and smart mobility have actually created more complexities and challenges to the emergence and institutionalisation of digital globalisation, and have been dealt with in an extensive manner throughout the article. This has been evident with uncovering of the huge transformations that have emerged across various nation-states such as the US, China, India, the EU, etc. The development and widespread use of AI have created greater possibilities of threats. The emergence of open-source software reduced cost, and greater accessibility of cyber technology has created a greater likelihood of attacks from non-state actors. This has increased the incidences of attacks, be it spam mails, phishing, social engineering-related attacks, identity theft or the mammoth DDoS attacks on smart cars. There should be a greater understanding, awareness, training, coordination and skilling of various actors and users in dealing with cyberattacks.

Unquestionably, these threats and challenges have created a greater need for countries to ensure greater cooperation and coordination among various states as well as non-state actors. The focus on the digital globalisation has vastly improved, and is very much evident with the global technological governance architecture emerging internationally. However, the emphasis of the multistakeholder approach, involving state and intergovernmental actors such as the US, China, the EU and India, has reached no consensus in creating an international regime that emphasises on the features of techno-globalisation. Rather, the international bandwagoning linked to dichotomous compartmentalisation has taken hold due to various reasons comprised in international politics, thereby fragmenting and fracturing the possibilities of coherent, interoperable and standardised systems to be established and remain in place.

The aspects of human security linkages that pertain to the development, institutionalisation and integration of AVs into society are very evident, especially in the context of digital globalisation and related challenges. The future of AVs and smart mobility is intricately linked to the level of integration into smart cities, and is inadvertently part of the Fourth Industrial Revolution. Among various aspects dealt with by the article, this is a very relevant one given the context of the current digitalisation and globalisation of the digital world. It is very important to theorise and conceptualise a human security approach to understanding the impact and implications of AVs. The article argues that countries must foresee as well as plan for a multitude of challenges and threats from the internet's growth and digitalisation in AVs and smart mobility systems. The implications on various communities, privacy and security of the state and individuals, and impact on other sectors such as agriculture, food distribution, IT and healthcare are all important facets of digital globalisation.

Universal acceptance of multistakeholderism around the globe for ensuring the creation of security architecture in dealing with threats has become a necessity. The AVs and the emergence of frontier technologies such as IoT, AI, big data and blockchain can and are transforming socioeconomic and political relations in various societies. However, the lack of an understanding of the interlinkages and transitioning that occur with the emergence of digital urbanisation or urban digitalisation has created more complexities that often unfold with newer challenges. This is evident with the US–China decoupling that has occurred internationally, as well as the domestic implications emerging along with it. The US–China trade-cum-technology war/conflict has been inadvertently founded based on narratives and arguments by and of the proponents of techno-nationalism, which has created a huge challenge for the emergence and institutionalisation of digital globalisation. This includes challenges such as cybersecurity and its variegated forms that create more challenges to the state and individuals, while creating issues in (the matter of) jurisprudence as well as technicalities in dealing with the threats and vulnerabilities that have been created in this regard. The internet and digitalisation will effectively provide opportunities and complexities for the state and individual, which will need to be dealt with in the coming years.

Acknowledgement

The authors would like to thank the Department of Science & Technology (DST), Government of India and the various stakeholders as well as participants for the input provided during the 'Brainstorming Session on Electric Vehicle Technologies' on April 20, 2022. The authors have been greatly benefitted from the inputs received from and academic interactions with faculties, staff and students at the Indian Institute of Technology Madras (IIT Madras), Mahatma Gandhi University, Jawaharlal Nehru University, Christ University, Indian Institute of Science (IISc) and various stakeholders of the Government of India. Further, the authors would also like to express gratitude to the reviewers of the journal for the extensive comments.

Funding

No external funding has been obtained from any agency with regard to the research conducted for, as well as the publication of, this article.

Conflict of Interest

The authors declare no potential conflict of interest for the publication of this manuscript.

References

Allied Market Research (AMR). 2018. Autonomous Vehicle Market. https://www.alliedmarketresearch.com/autonomous-vehicle-market. (Accessed 22 February 2022)

Audenhove, F. J. V., O. Korniichuk, L. Dauby, and J. Pourbaix. 2014. "The Future of Urban Mobility 2.0: Imperatives to Shape Extended Mobility Ecosystems of Tomorrow." *ArthurDLittle*. https://www.adlittle.com/sites/default/files/viewpoints/2014_ADL_UITP_Future_of_Urban_Mobility_2_0_Full_study.pdf. (Accessed 2 January 2022)

Balasubramanian, S. 2015. "PM Modi Rides Self-Driving Car in Masdar, World's First Zero-Carbon City." *NDTV*. https://www.ndtv.com/india-news/pm-modi-rides-self-driving-car-in-masdar-worlds-first-zero-carbon-city-1208011 (Accessed 2 July 2022)

Bates, O., C. Remy, C. Nash, and B. Kirman. 2019. "The future of techno-disruption in gig economy workforces: Challenging the dialogue with fictional abstracts." In *ACM International Conference Proceeding Series*. Nottingham: Association for Computing Machinery.

Batty, M. 2013. "Big Data, Smart Cities and City Planning." *Dialogues in Human Geography* 3 (3): 274–279.

Bildt, C. 2017. "Urbanisation 2.0." *Daily Star*. https://www.thedailystar.net/opinion/project-syndicate/urbanisation-20-1422592 (Accessed 12 July 2022)

Boulanin, V., and M. Verbruggen. 2017. *Mapping the Development of Autonomy in Weapon Systems*. Stockholm International Peace Research Institute. https://www.sipri.org/sites/default/files/201711/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf (Accessed 22 July 2022)

Broadhurst, R., and P. Grabosky. eds. 2005. *Cyber-Crime: The Challenge in Asia*. Hong Kong: Hong Kong University Press.

Brunette, D., and P. Eshel. 2020. "The Surprising Benefits of Self-Driving Trucks." *World Economic Forum*. https://www.weforum.org/agenda/2020/03/self-driving-trucks-will-change-the-world-more-than-you-might-think/#:~:text=Autonomous%20trucks%20will%20be%20safer,felt%20throughout%20the%20entire%20economy. (Accessed 22 June 2022)

Crunchbase. 2021. Build Query: Organizations. https://www.crunchbase.com/search/organizations/field/organizations/categories/drones. (Accessed 2 July 2022)

Ding, Z., B. Yang, Y. Chi, and L. Guo. 2015. "Enabling Smart Transportation Systems: A Parallel Spatio-Temporal Database Approach." *IEEE Transactions on Computers* 65 (5): 1377–1391.

Diwaker, P. 2018. "Kerala Floods and Drones." *Geospatial World*. https://www.geospatialworld.net/blogs/kerala-floods-and-drones/. (Accessed 12 July 2022)

ETHealthWorld. 2019. "Govt of Maharashtra, Zipline and SII Announce India's First Autonomous Instant Drone Delivery Service." *The Economic Times*. https://health.economictimes.indiatimes.com/news/medical-devices/govt-of-maharashtra-and-zipline-announce-indias-first-autonomous-instant-drone-delivery-service/71149101. (Accessed 2 December 2022)

European Commission (EC). 2019. *Factsheet: Artificial Intelligence for Europe*. https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe (Accessed 2 Mar 2022)

European Commission (EC). 2020. *Horizon 2020*. https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020 (Accessed 2 July 2022)

European Commission (EC). 2022. *EU Member States Sign Up to Cooperate on Artificial Intelligence*. https://ec.europa.eu/info/index_en (Accessed 12 June 2022)

European Defence Agency (EDA). 2016. *First EU Pilot Project in the Field of Defence Research Sees Grant Agreements Signed for €1.4 Million*. https://www.eda.europa.eu/info-hub/press-centre/latest-press-releases/2016/10/28/first-eu-pilot-project-in-the-field-of-defence-research-sees-grant-agreements-signed-for-1.4-million (Accessed 2 April 2022)

European Defence Agency (EDA). 2018. *Pilot Project EuroSWARM and SPIDER Activities Completed*. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/02/23/pilot-project-euroswarm-and-spider-activities-completed (Accessed 3 July 2022)

Filho, F. H. I., W. B. Heldens, Z. Kong, and E. S de Lange. 2020. "Drones: Innovative Technology for Use in Precision Pest Management." *Journal of Economic Entomology* 113 (1): 1–25.

Foucault, M. 1977. *Discipline and Punish: The Birth of the Prison.* Harmondsworth: Penguin.

German Aerospace Center (GAC). n.d. *TRAWA (Traffic Awareness*). https://www.dlr.de/fl/en/desktopdefault.aspx/tabid-1149/1737_read-50665/ (Accessed 2 March 2022)

Hebbar, P. 2018. "Top 6 AI Collaborations between NITI Aayog and Tech Giants in 2018." *AnalyticsIndiaMag*. https://analyticsindiamag.com/niti-aayog-ai-collaborations-2018/ (Accessed 2 July 2022)

Janai, J., F. Güney, A. Behl, and A. Geiger. 2020. "Computer Vision for Autonomous Vehicles." *Foundations and Trends in Computer Graphics and Vision* 12 (1–3): 1–308.

Kato, S., E. Takeuchi, Y. Ishiguro, Y. Ninomiya, K. Takeda, and T. Hamada. 2015. "An Open Approach to Autonomous Vehicles." *IEEE Micro* 35 (6): 60–68.

Korosec, K. 2018a. "Baidu Just Made its 100th Autonomous Bus Ahead of Commercial Launch in China." *Techcrunch*. https://techcrunch.com/2018/07/03/baidu-just-made-its-100th-autonomous-bus-ahead-of-commercial-launch-in-china/ (Accessed 12 July 2022)

Korosec, K. 2018b. "Daimler Can Now Test Self-Driving Cars on Public Roads in." *Techcrunch*. https://techcrunch.com/2018/07/06/daimler-self-driving-car-beijing/ (Accessed 1 July 2022)

Krishna, K. R. 2018. *Agricultural Drones: A Peaceful Pursuit*. NJ, USA: Apple Academic Press (Routledge).

Lang, F. 2020. Amazon Tribes Use Drones to Watch Over the Forest. Interesting Engineering'. https://interestingengineering.com/amazon-tribes-use-drones-to-watch-over-the-forest. (Accessed 2 July 2022)

Lee, J., J. Kim, and J. Seo. 2019. Cyber Attack Scenarios on Smart City and their Ripple Effects. In *2019 International Conference on Platform Technology and Service (PlatCon)*, pp. 1–5.

Librán-Embid, F., F. Klaus, T. Tscharntke, and I. Grass. 2020. "Unmanned Aerial Vehicles for Biodiversity-Friendly Agricultural Landscapes - A Systematic Review." *Science of the Total Environment* 732: 139204.

Lyon, D. 1993. "An Electronic Panopticon? A Sociological Critique of Surveillance Theory." *The Sociological Review* 41 (4): 653–678.

Lyon, D. 1994. *The Electronic Eye: The Rise of the Surveillance Society*. Cambridge: Polity Press/Blackwell.

Marx, G. T. 1988. *Undercover*. Berkeley: University of California Press: 1-280.

Marx, G. T. 2003. "What's New about the 'New Surveillance'? Classifying for Change and Continuity'." *Surveillance and Society* 1 (1): 9–29.

National Crime Records Bureau (NCRB). 2021. https://ncrb.gov.in/. (Accessed 2 July 2022)

Parkinson, S., P. Ward, K. Wilson, and J. Miller. 2017. "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges." *IEEE Transactions on Intelligent Transportation Systems* 18 (11): 2898–2915.

Press Information Bureau (PIB). 2018. MOVE: India's First Global Mobility Summit 2018 to be Inaugurated by the Prime Minister on 7th September. https://pib.gov.in/PressReleasePage.aspx?PRID=1545146 (Accessed 2 July 2022)

Press Information Bureau (PIB). 2021a. Shri Hardeep S. Puri inaugurates the Driverless Train Operations on the Pink Line of the Delhi Metro. https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1774960 (Accessed 2 July 2022)

Press Information Bureau (PIB). 2021b. Union Minister Dr Jitendra Singh calls for Global Scientific Collaboration for Bringing "Ease of Living" for Common Man. https://pib.gov.in/PressReleasePage.aspx?PRID=1741587 (Accessed 2 January 2022)

Ray, A. 2020. Food Delivery in India Via Drones? Zomato, Swiggy, Dunzo Can Start Testing, Says DGCA. https://www.livemint.com/companies/news/food-delivery-in-india-via-drones-zomato-swiggy-dunzo-can-start-testing-11591253543250.html. (Accessed 2 January 2022)

Reach Project. 2020. PURA: Addressing Rural Poverty in India. https://static1.squarespace.com/static/5769a0b5f7e0ab7b91a3362b/t/5e661fa7190266288c7c8be2/1583751082907/REACH2020-India-PURA-r4.pdf. (Accessed 2 January 2022)

Redican, S. J., and C. Zhang. 2020. "Canada: Payments on Wheels: Self-Driving Vehicles and the Future of Financial Services." *Mondaq*. https://www.mondaq.com/canada/financial-services/1018692/payments-on-wheels-self-driving-vehicles-and-the-future-of-financial-services?type=related. (Accessed 2 November 2022)

Reghunadhan, R. 2018a. "Cyber Threat Landscape of Digital India: A Critical Perspective." *Journal of Polity and Society* 10 (1&2): 37–50.

Reghunadhan, R. 2018b. "Political Economy of Digitalisation and (State)Neoliberalism in China with Special Reference to 'Made in China 2025'." *Research in Social Change* 10 (3): 22–43.

Reghunadhan, R. 2019. "Big Data, Climate Smart Agriculture and India–Africa Relations: A Social Science Perspective." In *IoT and Analytics for Agriculture*, edited by Pattnaik P. K., Kumar R., Pal S., and Panda S. N., Studies in Big Data, Vol. 63, Singapore: Springer Nature Singapore: 113–137.

Reghunadhan, R. 2020a. "Blockchain Technology and the Digital Society: Developments, Possibilities and Challenges." In *The Inclination of Library Professionals to Modern Tools in the Knowledge Era*, edited by Kumar V. V., and Savithry, T. K. Kottayam, Kerala: Kerala Library Association (KLA): 20–24.

Reghunadhan, R. 2020b. "Ethical Considerations and Issues of Blockchain Technology-Based Systems in War Zones: A Case Study Approach." In *Handbook of Research on Blockchain Technology*, edited by Krishnan S., Balas V., Golden J., Robinson Y., Balaji S., and Kumar R., Academic Press (Elsevier). 1–34.

Reghunadhan, R. 2022. *Cyber Technological Paradigms and Threat Landscape in India*. Singapore: Palgrave Macmillan: 1-134.

Reghunadhan, R., and A. E. Stanley. 2022. “Socioeconomic Impact of IoT on Agriculture: A Comparative Study on India and China.” In: *Internet of Things and Analytics for Agriculture*, *Volume 3*, edited by Pattnaik P. K., Kumar R., and Pal S., Studies in Big Data, Vol. 99. Singapore: Springer: 201-225.

Rolison, J. J., S. Regev, S. Moutari, and A. Feeney. 2018. “What are the Factors that Contribute to Road Accidents? An Assessment of Law Enforcement Views, Ordinary Drivers’ Opinions, and Road Accident Records.” *Accident Analysis and Prevention* 115: 11–24.

Sneha, P., N. Sinha, A. Durani, A. Patel, and A. Varghese. 2021. *Bureaucratic Indecision and Risk Aversion in India*. IDFC Institute. https://www.idfcinstitute.org/knowledge/publications/working-and-briefing-papers/bureaucratic-indecision-and-risk-aversion-in-india/ (Accessed 2 January 2022)

Stirling, R., H. Miller, and E. Martinho-Truswell. 2018. Government AI Readiness Index 2017. https://www.oxfordinsights.com/government-ai-readiness-index (Accessed 2 May 2022)

Tomtom. 2020. Traffic Index 2020. https://www.tomtom.com/en_gb/traffic-index/ranking/.

United Nations (UN). 2014. World’s Population Increasingly Urban with More than Half Living in Urban Areas. http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html (Accessed 2 October 2022)

United Nations Development Programme (UNDP). 1994. *Human Development Report 1994*. New York: Oxford University Press: 1-226.

United Nations Development Programme (UNDP). 2000. *Human Development Report 2000*. New York: Oxford University Press: 1-290.

United Nations Development Programme (UNDP). 2001. *Human Development Report 2001*. New York: Oxford University Press: 1-264.

United Nations Development Programme (UNDP). 2009a. *Human Development Report 2009*. New York: Oxford University Press: 1-217.

United Nations Development Programme (UNDP). 2009b. *Human Security in Theory and Practice: An Overview of the Human Security Concept and United Nations Trust Fund for Human Security*. New York: Human Security Unit: 1-79.

United Nations Development Programme (UNDP). 2019. *Human Development Report 2019*. New York: Oxford University Press: 1-350.

United Nations Development Programme (UNDP). 2020. *Human Development Report 2020*. New York: Oxford University Press: 1-22.

White, M. A., and Garry D. B. 2010. *The Management of Technology and Innovation: A Strategic Approach*. New York: Cengage Learning: 1-388.

Wismonsky, H. & Shany, Y. (2016). Cyber Threats to ‘Smart Cars’ – The Legal Response. *The Federmann Cyber Security Research Center – Cyber Law Program*. https://csrcl.huji.ac.il/smart-cars (Accessed on 12 April 2022).

Yağdereli, E., C. Gemci and A. Z. Aktaş. 2015. “A Study on Cyber-Security of Autonomous and Unmanned Vehicles.” *The Journal of Defense Modeling and Simulation* 12 (4): 369–381.

Zipline. 2021. Delivery at the Speed of Life. https://flyzipline.com/. (Accessed 2 May 2022)