Journal of Economic Policy Reform

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/gpre20

Addressing Policy Challenges of Disruptive Technologies

Araz Taeihagh

To cite this article: Araz Taeihagh (2023): Addressing Policy Challenges of Disruptive Technologies, Journal of Economic Policy Reform, DOI: 10.1080/17487870.2023.2238867

To link to this article: https://doi.org/10.1080/17487870.2023.2238867

Published online: 27 Jul 2023.

JOURNAL OF ECONOMIC POLICY REFORM
https://doi.org/10.1080/17487870.2023.2238867

Routledge
Taylor & Francis Group

OPEN ACCESS

Addressing Policy Challenges of Disruptive Technologies

Araz Taeihagh

Lee Kuan Yew School of Public Policy, National University of Singapore, Singapore, Singapore

ABSTRACT
This special issue examines the policy challenges and government responses to disruptive technologies. It explores the risks, benefits, and trade-offs of deploying disruptive technologies, and examines the efficacy of traditional governance approaches and the need for new regulatory and governance frameworks. Key themes include the need for government stewardship, taking adaptive and proactive approaches, developing comprehensive policies accounting for technical, social, economic, and political dimensions, conducting interdisciplinary research, and addressing data management and privacy challenges. The findings enhance understanding of how governments can navigate the complexities of disruptive technologies and develop policies to maximize benefits and mitigate risks.

ARTICLE HISTORY
Received 17 July 2023
Accepted 17 July 2023

KEYWORDS
Disruptive technologies; emerging technologies; technological disruption; regulation; governance, policy

JEL Classification
O00; O32; O33; O38; K20; L50; L88; L98

Introduction

The proliferation and rising pace of development of disruptive technologies such as generative AI, autonomous systems, big data, blockchains and the Internet of Things pose challenges to governments that must balance their positive effects with their potential negative consequences and harms (Cagigas et al. 2023; Pande and Taeihagh, 2023).

On the one hand, these disruptive technologies have the potential to increase efficiency, productivity, and convenience, promising a surge in economic growth, innovation, and accessibility. On the other hand, the rapid pace of development of these technologies often surpasses our ability to understand the implications of these technologies, which leads to significant risks and unintended consequences. These issues range from data privacy and security in big data applications (Wilson and Hinnant, this issue), to questions about the future of work, how AI and autonomous systems will displace low and high-skilled workers and the social and economic ramifications this brings (Clifton, Glasmeier, and Gray 2020). Disruptive technologies are bringing complex ethical dilemmas and have the potential of increasing the social divide (Tan, Taeihagh, and Tripathi 2021; World Bank 2018).

Addressing these policy challenges would require a comprehensive approach to address technical problems and protect citizens' livelihoods and rights. These include promoting fair labour practices and support for upskilling and reskilling in the face of AI,

CONTACT Araz Taeihagh spparaz@nus.edu.sg; araz.taeihagh@new.oxon.org

enhancing data protection laws and promoting the improvement of personal data storage and handling and preventing data breaches, along with ensuring equitable access to these technologies.

Given the high technological and economic uncertainties, these are difficult objectives to achieve. Due to a lack of information about these technologies and the networked nature of these technologies, traditional command and control and incentive-based policy tools are ill-equipped to deal with them. Often few companies dominate the market and stifle competition. This "winner takes all" dynamic not only favours a few dominant players but also reduces the number of choices available to the consumer, increases the risk of monopolistic practices and can lead to increased influence over standard-setting organisations. There are difficulties in engaging stakeholders and having inclusive outcomes due to the complex nature of these technologies, which makes consensus-building difficult. Many stakeholders might not have the necessary expertise to understand these technologies, further exacerbating the problem.

To overcome these challenges, governments must adopt an adaptive and proactive approach (Janssen and Van Der Voort 2016; Tan and Taeihagh 2021) and increase transparency and collaboration by drawing from public consultations and partnerships with academia, industry and civil society to benefit from a wide range of experiences and expertise to better understand disruptive technologies and address the challenges they bring due to information asymmetries, policy uncertainty and power dynamics (Taeihagh, Ramesh, and Howlett 2021). As such it is important to uphold social values and rights while striving to maximise benefits from disruptive technologies and build the capacity of the stakeholders to better understand and navigate the complexities of disruptive technologies (Lee, Malerba, and Primi 2020).

Overview of the special issue articles

The articles in the special issue examine addressing policy challenges of disruptive technologies through case studies and comparative analyses. They address gaps in the literature pertaining to understanding the risks, benefits, and trade-offs of deploying disruptive technologies in various applications and domains. They explore the efficacy of traditional governance approaches and explore new regulatory and governance approaches that have been adopted or ought to be adopted to address the complexity of deploying disruptive technologies given their uncertainties, risks and unintended consequences and derived key lessons to facilitate policy learning. Below, a summary of the articles in the special issue is presented.

Cyberspace and the protection of critical national infrastructure (Weiss and Biermann, 2023)

Critical national infrastructures (CNI), such as energy, financial services, and transportation, are the foundations of modern societies. The protection of CNIs is necessary from a national security perspective as well as an economic perspective. Since security is the domain of the government and market provision involves the private sector, the protection of CNI requires the active participation of both the government and the private sector.

In Europe, a general standard model of governing the cybersecurity of CNIs can be observed. This entails the establishment of a new agency or empowering existing agencies mandated to protect CNI. However, there are variations in how such agencies approach cybersecurity protection. While some governments employ hierarchical models of CNI governance, others use a more arms-length coordinative approach. Using two opposite cases of France and the UK, this article argues that national variations in CNI cybersecurity designs can be explained by a) the historical institutions of the respective countries; and b) the nature of the threats themselves.

To elaborate, the authors argue that historically market-capitalist states will employ an arms-length approach to cybersecurity governance by providing greater independence and flexibility to the vital operators (VOs). At the same time, state-capitalist countries will pursue a more centralized and hierarchical mode of governance where few agencies are given regulative powers over private VOs. The former model requires a greater degree of coordination amongst various actors involved in the CNI sector, while the latter model requires the creation of a powerful enforcement agency that has coercive powers to impose and administer minimum cybersecurity requirements.

On the nature of the threats, the authors argue that two specific cybersecurity-related problems can be distinguished: a) diffused risks related to the vulnerabilities of the CNI infrastructure that require better coordination and infrastructure improvement amongst involved agencies; and b) threats posed by specific actors such as hackers, cybercriminals, and other malicious actors that require target protection and rival actor neutralization. The claim is that governments employ hierarchical forms of governance mechanisms to protect against actor-centred threats while they require coordination-related governance mechanisms to address security risks. Even then, a historically state-capitalist state is comparatively still more likely to employ hierarchical governance models on security risks, while market capitalists are more likely to employ horizontal governance forms for threats.

The authors conduct a structured comparison between the UK and France by examining official documents, government reports and other legal documents from 2010 to 2018 and comparing the two countries' governance approaches. They examine the approaches taken by their respective CNI-related cybersecurity agencies, the French Network and Information Security Agency (ANSSI) and the British National Cyber Security Centre (NCSC) and compare their protection capacity and policy approach styles. The authors find that, CSI protection in France takes a highly centralized approach. The ANSSI is the exclusive national authority in charge of cyber protection, has a staff of six hundred people and an annual budget of over one hundred million euros. The agency was created in 2009 and directly reports to the Prime Minister's office. The NCSC, however, only became a centralized agency for cyber protection in 2016 due to the EU Network and Information System (NIS) directive and was otherwise a patchwork of various agencies.

The authors also argue that although both countries involve the private sector to manage diffuse risks, the UK's reliance on the private sector is greater. In France, the ANSSI is empowered by the Military Programming Act and the Critical Infrastructures Information Protection (CIIP law) to require VOs to strengthen their security system. VOs are further required to notify of any cyber incidents, to enforce minimal standards, and oblige by the hierarchical monitoring mechanism under the law. The UK, meanwhile, relies on financial incentives and guidance to induce private and public sectors to improve their cybersecurity infrastructure and the Centre for the Protection of National Infrastructures (CPNI) plays an advisory and facilitative role in this regard. A similar approach can be noticed in risk management, where the ANSSI relies on government certification to ensure the quality of risk management, while the UK provides advisory services to guide the private sector towards public-private or private certification services.

Overall, the article shows that historical institutions are crucial determinants of policy designs, even for emerging technologies such as the cybersecurity of CNI. The author suggests that effective CNI protection requires collaboration between public and private actors to address the disruptive nature of cyber threats.

Competing perspectives on the big data revolution: a typology of applications in public policy (Wong and Hinnant 2023)

The use of big data in government has been fraught with contradictions. Proponents of the technology argue that big data can be used for evidence-based policymaking for better service delivery and reduced cost through digitalization. Big data has also been considered useful for measuring and evaluating performances, collaboration between citizens and the state, and better coordination amongst policymakers by encouraging information sharing. However, the use of big data has also been associated with various negative externalities, such as the greater potential for algorithmic discrimination, greater digital divide and the consequent digital inequality, and privacy threats. Given the high level of expertise required, its usefulness has also been questioned because of the potentially low capacity of data utilization amongst policymakers.

Previous experiences from ICT adoption have shown that successful mobilization of technology, both in private and public organizations, is contingent upon a wide variety of factors that are both exogenous and internal to the organizations. Quite often, even in established technologies, organizations need to adapt, modify, or transform such technologies before applying them internally. The authors argue that the benefits and costs associated with adopting such technologies (e.g. big data) are moderated by a set of internal and external factors under which organizations operate. In the context of Big Data, they examine such factors under political, economic, social, organisational, values and ethics, and regulatory dimensions.

The authors then dig into the last dimension, which is regulation, and attempt to understand how, given a country's regulatory capacity and nature, different approaches to technology use might evolve. While they admit that they have deliberately ignored multiple other dimensions along which such analysis can be done, for this study, they identify two areas of classification: a) regulatory orientation; and b) information reciprocity. Regulatory orientation refers to the degree of empowerment provided to the public or the private sector in the regulations that govern data in the country. The orientation depends on the existing political economy and can determine policy approaches to important issues such as privacy, personal freedom, and autonomy in data management. More privacy-related regulations, for instance, empower the private sphere and weakens the government's influence on data management. Similarly, information reciprocity refers to the incentive structure that facilitates information sharing across various private and public actors that generate and use the data. Information reciprocity is often a function of the degree of trust and partnership between such actors.

Based on the two variables, the authors derive a typology of the application of big data, which helps in understanding the different applications of big data in public policy and their potential benefits and drawbacks. The authors categorise the big data applications and provide examples as state-centric (public and information reciprocity, e.g. US's Patriot Act), big brother (public and information non-reciprocity, e.g. China's social credit system), society-centric (private and information reciprocity, e.g. EU's GDPR) and fragmented big data (private and information non-reciprocity, e.g. Hong Kong's smart city development initiative). This highlights the importance of context and nature of the big data application as well as the need for appropriate levels of regulations and provision of ethical guidelines to ensure the responsible use of such technology. The article concludes by saying that typologies and classifications developed in the study should be used to set up testable hypotheses and can enrich empirical work of the future.

An integrated complex adaptive governmental policy response to cyber threats (Porter and Tan, 2023)

Technologies of today are characterized by a high degree of complexity. This is truer for cyber threats, characterized by various specific challenges. Cyber threats are associated with a high degree of uncertainty and unpredictability. Since the nature of threats is constantly evolving, and so are the anonymous actors posing these threats, designing linear problem-solving mechanisms to address cybersecurity challenges is ineffectual. For instance, in the case of ransomware as a service (RaaS), the lead actor is often a service provider that enables primary threat actors to carry out ransomware attacks in return for a share of ransomware. Cyber threats are also characterized by a potential multiplicity of origins of threats. The scope of cyber threats can be at global, national, local, or individual levels, where scope refers to the location of the source of threats and the location of the potential victims of threats.

These specificities of cyber threats mean that governance-related responses to these challenges must display complex adaptive designs. The authors discuss policy options available to governments to address cyber threats and argue for an adaptive design approach, as linear planning and policy design requires that policymakers anticipate the nature of the problem at hand and the desired outcome and create a path of change through the policy. Under conditions of high degree of uncertainty and complexity pertaining to cyber threats, such design thinking often fail. Therefore, the authors identify specific characteristics of complex policy systems to tackle this issue: self-organization, feedback loops, experimentation, and adaptation. Together, these four features permit connectivity between actors, openness to external knowledge absorption and assimilation, non-linear and iterative problem-solving, and experimentation.

The authors argue that cyber threats are complex problems to address due to the presence of these four properties. In particular, the authors claim that any response to cyber threats must be aimed at enhancing the coordinated decentralized capacity for experimentation and resilience. Three elements of this response need attention. Coordinated decentralization capacity requires abilities related to self-organization, involvement of a multitude of actors, and synchronicity in approaches between various subsystems and actors. The role of the government is more of an organizer or an activist rather than a policy monopolist or a bystander. Resilience requires the capacity of the system to bounce back after perturbations, and experimentation entails creative thinking and non-traditional approaches to problem-solving.

Response to the locational complexity also requires approaching challenges at all levels simultaneously, recognizing the interrelatedness between any emerging policy design. To elaborate, it is important to design international norms to reduce global-scale threats and mechanisms to facilitate international support to protect against global threats. At a local level, governments must ensure sufficient support to the private sector to enable them to invest in cybersecurity. At the same time, creating a collaborative environment that can promote information and expertise sharing and coordination between actors across various locations is also vital. Similarly, trainings, awareness campaigns, and regulations against cybercrimes can contribute to better protection at the individual level.

The authors use the case of the 2007 cyberattack in Estonia to illustrate how complex policy design can help governments approach potential problems related to cyber threats. In 2007, a distributed denial-of-service (DDOS) was carried out in Estonia, targeting government bodies, ministries, banks, media sources, and other private companies.

The Estonian approach to this attack and its subsequent reforms highlight the complex policy design system's strengths, especially its coordinated decentralized capacity for experimentation and resilience. The Estonian Government created the Estonian Computer Emergency Response Team (CERT) in 2006. CERT was a national-level coordinating body responsible for coordinating various public and non-public agencies within the country but simultaneously with close relationships with international and other national cybersecurity agencies. Various initiatives have been undertaken within Estonia to prepare the country against such attacks. In 2006, the Estonian government signed an MOU with firms operating in critical sectors to share information on cyber threats. Beyond Estonia, the country had signed the Council of Europe's Convention on Cybercrime in 2001 and had established a cyber defence centre of excellence as a member of NATO.

After the cyberattack, the government actively pursued information sharing and coordination between the public and private sectors. It also established a voluntary Estonian Defence League's Cyber Unit that included programmers conducting regular training and exercises for the public and private sectors. It created various collaboration platforms, such as the cybersecurity in AI accelerator and the Cyber Command (2019), which consisted of active membership from experts from private, military, and public domains. The government is also actively working with educational institutions to organize awareness programs and competitions to generate skilled human resources in the sector. Beyond Estonia, the government has also established a cyber partnership agreement with the US and worked with NATO on establishing the Cooperative Cyber Defence Centre of Excellence.

Therefore, given the complex nature of challenges, the government's efforts have focused on global, national, local, and individual levels, focusing on elements of coordinated decentralized capacity for experimentation and resilience. The authors call for a comprehensive and adaptive approach to respond to cyber threats. Built not only based on technical measures but also including broader institutional changes such as building partnerships and increasing coordination among the public and private sectors.

Navigating the governance challenges of disruptive technologies: insights from regulation of autonomous systems in Singapore (Pande and Taeihagh, 2023)

Autonomous systems (AS) can potentially lead to a greener, more efficient, and more productive economic future. However, at present, various operational, legal, economic, social, and ethical challenges are associated with the governance of AS (Pande and Taeihagh, 2023). Addressing these challenges is crucial for creating a conducive environment for fruitful utilization of AS. Regulating new technologies is always difficult, given the pacing problem associated with them. The complexities of the AS, however, make their regulation more difficult. First, inherent uncertainties associated with the operations of AS limit the information available to make assessments about their risks ex-ante difficult. Second, the risks of AS differ as per their form and application. AS is a broader umbrella term under which different forms of systems operate. Autonomy and the level of risks presented by different AS systems are dissimilar. At the same time, the same AS might present different risks depending on the environment in which they are applied (Pande and Taeihagh, 2023).

It then becomes important to understand how policymakers have attempted to wrestle with these two challenges to design regulatory frameworks governing AS to promote their experimentation and application. The authors take the case of Singapore to understand the specific challenges associated with the governance of various AS and the regulatory frameworks that can address these challenges without constraining the inherent need for application and experimentation.

The authors identify operational, legal, economic, social, and ethical challenges for autonomous vehicles, unmanned aerial vehicles, industrial robots, and personal care robots. They then specify how Singapore has created regulations to address these challenges for various AS. The study describes the specific peculiarities associated with the four technologies across the five types of challenges and then identifies steps taken to minimize associated risks. The authors identify various regulatory measures undertaken by the Singapore government. Such measures included mandatory human supervision, designating responsibility for control, the existence of a stopping mechanism, creation of standards for data collection, storage, protection, and use, among others (Pande and Taeihagh, 2023).

The study highlights that the Singapore government's response has addressed most of the generic and domain-specific challenges associated with AS. The authors argue that Singapore has adopted a control-oriented strategy that has successfully limited the risks of the technology while making the country a test-bed for experimentation and use. This has meant that policymaking has paid special focus on ensuring the government regularly reviews and updates its regulations, that experimentation and policymaking have been a coordinated effort which involves the participation of a wide variety of stakeholders, and that sufficient attention is paid to safety concerns to ensure lives and livelihoods are protected. The authors highlight that there is room for further developments in response to ethical dilemmas and social challenges associated with adopting AS.

Additionally, the authors argue for stronger and clearer liability-related regulations and stress the need for the regulations to be more frequently revisited and revised to adapt to the rapid pace of technological developments (Pande and Taeihagh, 2023). The authors suggest that governments can take steps to introduce experimental regulations and sunset clauses that permit flexibility in use and encourage experimentation while minimizing risks.

The article highlights governments' critical role in navigating disruptive technologies' challenges and calls for a comprehensive and proactive approach not only through regulatory measures but also through fostering collaboration and stakeholder engagement to promote responsible innovation.

Addressing policy challenges of disruptive technologies: key takeaways

What are some of the common challenges that disruptive technologies bring about that necessitate policy responses from governments? Based on the articles in the special issue, some of the common themes that emerge in relation to addressing the challenges of disruptive technologies include (see Table 1):

Emphasis on the role of the government

All the articles underscore the critical role of the government in addressing the challenges posed by disruptive technologies. They emphasise that beyond deploying direct policy measures such as regulations and law enforcement, there is a need to promote awareness, promote collaboration and partnerships among the stakeholders, and encourage ethical and responsible innovation.

Need for comprehensive policies

The articles highlight the need for comprehensive policies that consider the complexity and interconnectedness of disruptive technologies. They emphasise that the policies should not only focus on the technical aspects of these technologies but also their social, economic, and political dimensions.

Adaptive and proactive approach

Due to the rapid pace of technological developments and the complexity of technological systems that disruptive technologies create, controlling and regulating them all in one go is difficult. Articles highlight various types of risks (cyber threats, data management, privacy, discrimination, ethical dilemmas, etc.) and the need for anticipating potential threats/challenges and developing strategies to address them before they occur. They advocate taking an adaptive approach, actively monitoring the situation and having the flexibility to continuously update policies in response to evolving risks and changes to the circumstances. They highlight the need to address the skills and capacity gaps in the public sector and among stakeholders.

Table 1. Common themes in addressing the policy challenges of disruptive technologies.

Article	Role of Government	Need for Comprehensive Policies	Adaptive and Proactive Approach	Interdisciplinary Research	Data Management and Privacy
Cyberspace and the protection of critical national infrastructure. (Weiss and Biermann, This Issue)	Emphasizes the government's role in protecting CNI from cyber threats.	Calls for comprehensive policies that address the complexity of cyberspace and the potential threats to CNI.	Highlights the complexities of cyberspace and advocates for a proactive approach to protecting CNI with policies that can adapt to the rapidly changing landscape of cyberspace.	The paper's approach implies a need for interdisciplinary research that combines a technical understanding of cyberspace with policy and regulatory expertise.	Indirectly touches on this theme, as protecting CNI in cyberspace would involve managing and securing data.
Competing perspectives on the Big Data revolution (Wong and Hinnant, This Issue)	Discusses the government's role in regulating the use of Big Data and ensuring that it is used responsibly and ethically.	Calls for comprehensive policies that address the various aspects of the Big Data applications, including data privacy and management, and data-driven decision making.	Highlights the complexity of Big Data applications and suggests that governments must proactively address the challenges and opportunities of Big Data.	Calls for further research to explore the potential applications and implications of the Big Data through interdisciplinary research.	Discusses the challenges of managing and protecting the vast amounts of data collected, stored, and generated by Big Data technologies.
An integrated complex adaptive governmental policy response to cyber threats (Porter and Tan, This Issue)	Emphasizes the government's role in responding to cyber threats.	Argues for comprehensive policies that can address the complexity of cyber threats and the interconnectedness of the digital ecosystem.	Discusses the complexity of the digital ecosystem and proposes an adaptive policy response to cyber threats, suggesting that policies must be flexible and able to respond rapidly.	Calls for an interdisciplinary approach to understanding and addressing cyber threats.	The theme of data management and privacy is inherent in discussing cyber threats and the need for secure digital infrastructure.
Navigating the governance challenges of disruptive technologies: (Pande and Taeihagh, This Issue)	Underscores the role of government in regulating disruptive technologies such as AS and ensuring the balance between innovation and protecting the citizens from risks.	Discusses the need for comprehensive policies to address the operational, legal, economic, social, and ethical challenges that AS pose.	Suggests that governments must be proactive in addressing the challenges of disruptive technologies (AS in particular) and flexible in adapting to their rapid evolution.	Calls for further research to explore the governance challenges of AS and their regulation.	The data management and privacy theme are relevant in the context of AS, which involve collecting and using large amounts of sensor data.

Need for interdisciplinary research

The need for interdisciplinary research to understand and address the challenges posed by disruptive technologies is emphasised by all of the articles in the special issue due to the complex nature of these technologies. Aside from a better understanding of the technical aspects of these technologies, there is a need for a deeper understanding of their economic, political, legal, social, and ethical implications. While these technologies can potentially enhance citizen engagement and service delivery, they can also create safety risks and result in discrimination, inequality and digital divide.

Data management and privacy

Disruptive technologies often rely on the collection, storage and use of large amounts of data, and there is a need to highlight the importance of data literacy and regulations for data protection. Wong and Hinnant, (2023) and Pande and Taeihagh, (2023), in particular, emphasise the challenges related to data management and privacy regarding the use of Big Data and Autonomous systems, while other papers in the special issue indirectly touch on this theme.

The common themes highlighted in Table 1 emphasise the role of government and the need for comprehensive and adaptive policies to address the challenges of disruptive technologies. Additionally, the need for interdisciplinary research to unpack the risks and impacts of these technologies, along with improving data management and privacy, is stressed.

Acknowledgments

Araz Taeihagh is grateful for the funding support provided by the Lee Kuan Yew School of Public Policy, National University of Singapore. The special issue editor would like to thank Professor Judith Clifton, the editor of the Journal of Economic Policy Reforms and all the anonymous reviewers for their constructive feedback and support for this special issue on Addressing Policy Challenges of Disruptive Technologies. A special thanks to Hazel Lim, Devyani Pande, Siying Tan and Shaleen Khanal of the Policy Systems Group for their support in organising this special issue.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Lee Kuan Yew School of Public Policy, National University of Singapore.

ORCID

Araz Taeihagh http://orcid.org/0000-0002-4812-4745

References

Cagigas, D., J. Clifton, D. Diaz-Fuentes, M. Fernández-Gutiérrez, and C. Harpes. 2023. “Blockchain in Government: Toward an Evaluation Framework.” *Policy Design and Practice* 1–18. https://doi.org/10.1080/25741292.2023.2230702.

Clifton, J., A. Glasmeier, and M. Gray. 2020. “When Machines Think for Us: The Consequences for Work and Place.” *Cambridge Journal of Regions, Economy & Society* 13 (1): 3–23. https://doi.org/10.1093/cjres/rsaa004 .

Janssen, M., and H. Van Der Voort. 2016. “Adaptive Governance: Towards a Stable, Accountable and Responsive Government.” *Government Information Quarterly* 33 (1): 1–5. https://doi.org/10.1016/j.giq.2016.02.003.

Lee, K., F. Malerba, and A. Primi. 2020. “The Fourth Industrial Revolution, Changing Global Value Chains and Industrial Upgrading in Emerging Economies.” *Journal of Economic Policy Reform* 23 (4): 359–370. https://doi.org/10.1080/17487870.2020.1735386.

Pande, D., and A. Taeihagh. 2023. “Navigating the Governance Challenges of Disruptive Technologies: Insights from Regulation of Autonomous Systems in Singapore.” *Journal of Economic Policy Reform* 1–22. https://doi.org/10.1080/17487870.2023.2197599.

Porter, T., and N. Tan. 2023. “An Integrated Complex Adaptive Governmental Policy Response to Cyberthreats.” *Journal of Economic Policy Reform* 1–15. https://doi.org/10.1080/17487870.2022.2125390 .

Taeihagh, A., M. Ramesh, and M. Howlett. 2021. “Assessing the Regulatory Challenges of Emerging Disruptive Technologies.” *Regulation & Governance* 15 (4): 1009–1019. https://doi.org/10.1111/rego.12392.

Tan, S. Y., and A. Taeihagh. 2021. “Adaptive Governance of Autonomous Vehicles: Accelerating the Adoption of Disruptive Technologies in Singapore.” *Government Information Quarterly* 38 (2): 101546. https://doi.org/10.1016/j.giq.2020.101546.

Tan, S. Y., A. Taeihagh, and A. Tripathi. 2021. “Tensions and Antagonistic Interactions of Risks and Ethics of Using Robotics and Autonomous Systems in Long-Term Care.” *Technological Forecasting and Social Change* 167:120686. https://doi.org/10.1016/j.techfore.2021.120686.

Weiss, M., and F. Biermann. 2023. “Cyberspace and the Protection of Critical National Infrastructure.” *Journal of Economic Policy Reform* 1–18. https://doi.org/10.1080/17487870.2021.1905530.

Wong, W., and C. Hinnant. 2023. “Competing Perspectives on the Big Data Revolution: A Typology of Applications in Public Policy.” *Journal of Economic Policy Reform* 1–15. https://doi.org/10.1080/17487870.2022.2103701.

World Bank. (2018). *World Development Report 2019: The Changing Nature of Work*. The World Bank. https://www.worldbank.org/en/publication/wdr2019.