Government and Opposition (2025), **60**, 751–772
doi:10.1017/gov.2024.31

Government & Opposition

ARTICLE

Digital Authoritarianism and the Global Technology Industry: Evidence from Iran

Dara Conduit

Department of Social and Political Sciences, University of Melbourne, Melbourne, Australia
Email: dconduit@unimelb.edu.au

(Received 27 February 2024; revised 3 October 2024; accepted 16 October 2024; first published online 7 January 2025)

Abstract

The purchase of commercial spyware by at least 43 authoritarian states has drawn attention to the links between the international private technology trade and autocrats. This article sits at the intersection of the literatures on the international relations of authoritarian regimes, digital authoritarianism and the political economy of authoritarianism, asking, what impacts, if any, do the foreign technology trade relations of authoritarian regimes have on authoritarian resilience? Building a four-mechanism model to explain the interaction between the private technology trade and digital authoritarianism, the article then tests the model on a case study of Iran. It argues that while global technology companies lack the ideological or geopolitical interests that drive the engagement between authoritarian regimes and foreign states, an intense overlap in interests still exists between profit-hungry private technology companies and technology-hungry regimes. This facilitates the establishment of mutually beneficial relationships that contribute to authoritarian resilience and survival, however inadvertently.

Keywords: surveillance arms trade; Middle East; authoritarianism; political economy of authoritarianism; authoritarian economics

Authoritarian regimes today bear little resemblance to those of the late Soviet era, with William Dobson (2012: 4–5) arguing that 'modern authoritarians have successfully honed new techniques, methods, and formulas for preserving power, refashioning dictatorship for the modern age'. Over the past two decades, advanced digital technology has played a significant role in this autocratic transformation, leading to the emergence of a phenomenon known as 'digital authoritarianism' (Dragu and Lupu 2021; Polyakova and Meserole 2019). Yet building and maintaining this advanced digital capacity – particularly in the face of evermore sophisticated technological threats from opponents at home and abroad – has required autocrats to continuously develop or acquire new technology. In practice, this has seen private technology companies become key suppliers to authoritarian regimes. Perhaps the best example of this is China, where the state's

© The Author(s), 2025. Published by Cambridge University Press on behalf of Government and Opposition Ltd. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

inability to meet its technology needs in-house meant that domestic private sector became essential to upgrading the state's 'coercive capacity' (Huang and Tsai 2022: 7). Indeed, Kevin Liu (2019: 3) identified the emergence of a 'commercial-state surveillance complex, wherein the state and tech-giants like Tencent work hand-in-hand to engineer user behaviour and public discourse'. But China is an outlier case: most other authoritarian states do not have an advanced domestic technology sector from which to draw. To Jennifer Pan (2017), this poses a fundamental limitation on such states' ability to achieve Chinese-style content controls.

Yet as authoritarian regimes around the world grow in sophistication and technological ambition, there is much evidence to suggest that the global technology sector is filling technology gaps. By 2021, at least 43 authoritarian states had deployed private-sector-produced spyware (Feldstein 2021: 82), exemplifying the significant overlap that was emerging between the commercial interests of foreign technology companies and the survival-driven goals of their authoritarian clients. It was leading to the unprecedented international outsourcing of state security infrastructure, giving the private sector a role in some of the most politically sensitive parts of contemporary authoritarian regimes. This complex, shadowy and little understood set of authoritarian regime–global technology company relationships prompts this article to ask, what impacts, if any, do the foreign technology trade relations of authoritarian regimes have on authoritarian resilience?

This article argues that the answer to this question sits at the intersection of three strands of the literature. The first is the rapidly expanding body of work on 'digital authoritarianism' (Dragu and Lupu 2021; Erixon and Lee-Makiyama 2011; Polyakova and Meserole 2019; Shukri 2023), which this study defines as the autocratic use of technology in the pursuit of authoritarian resilience and survival. It has provided autocrats with new avenues through which to shore up their rule. Scholarship has examined aspects of the phenomenon ranging from the international diffusion of technology and technology policy (Codreanu 2022; Kerr 2018; Polyakova and Meserole 2019), the failure of digital counter-revolutions (Cebul and Pinckney 2021) and transnational digital repression (Fatafta 2021). It has led to increasing recognition that technology can strengthen authoritarian regimes (Foreign Affairs 2019; Gohdes 2020; Morozov 2011; Qin et al. 2017) and reduce the risk of protests (Frantz et al. 2020). Some scholars have argued that authoritarianism has been fundamentally changed by technology (Lamensch 2021; Schlumberger et al. 2024).

However, very little attention has been given to understanding how authoritarian regimes are procuring the infrastructure of digital authoritarianism, and in particular the international aspects of this beyond direct authoritarian state-to-state collaboration (Morgus 2019; Polyakova and Meserole 2019; Sinkkonen and Lassila 2022) or how such collaborations contribute to this so-called change in the nature of authoritarianism. This is despite the fact that another group of scholars has drawn direct links between the way that autocrats leverage their foreign relations to enhance the resilience of their regimes. This is the second body of literature from which this article draws, including works that examine the impact of bilateral relationships such as those between authoritarian regimes and 'black knights' (Levitsky and Way 2010) who act as 'guardians of autocracy or challengers of democracy in specific contexts' (Tolstrup 2015: 676), and those that study ties between autocrats and regional or international organizations that may facilitate

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

'autocratization' (Cottiero and Haggard 2023; Debre 2021). Indeed, a connection has been established between authoritarian survival and relations with foreign states (Tansey 2016; Tolstrup 2015), regional organizations (Debre 2021) and even diasporas (Baser and Ozturk 2020). As Oisin Tansey (2016: 5) noted, international relationships 'contribute to a range of aspects of authoritarian politics, making it more likely that authoritarian incumbents will resort to authoritarian practices, [and] contributing to the implementation of those practices'. But while this literature provides important insight into the foreign connections of authoritarian states and draws a direct line between those connections and authoritarian resilience, private technology companies form a very different type of international sponsor to the foreign state actors or multilateral bodies that have predominantly been observed.

This article therefore also draws on works on the political economy of authoritarianism. This is an important piece of the puzzle because, as Tansel (2018: 210) noted, authoritarian regimes have embraced neoliberal policies, increasing 'the scope and pace of commodification and restructured the state's regulatory and distributive roles'. This has seen the entrance of private corporations into the authoritarian political-economic milieu: actors that are often guided by different interests to those of the regime, including profitability, responsibilities to shareholders and sometimes global corporate responsibility (Ratner 2001). Although some private corporations are ideologically driven, such ideologies rarely exactly match those of the states with which they do business. Relationships with authoritarian regimes can nonetheless flourish amid a narrow, opportunistic overlap of interests: Guillermo O'Donnell (1978) noted decades ago that authoritarian agendas and international capital often complement one another. For example, private arms manufacturers might sell weapons to authoritarian regimes and be reasonably aware of how such arms will be used (Stavrianakis 2017, 2023), but their decision to engage is more likely driven by commercial considerations than an ideological commitment to regime survival. Regime survival might nonetheless be essential to guaranteeing ongoing business. The handful of works on the political economy of digital authoritarianism have noted the continuation of this overlap. Observing Cambridge Analytica, Meta and the NSO Group, Koray Saglam (2022: 2) argued that 'tech companies are also incentivized to fully exploit the commercial potential of "the digital", irrespective of social or political externalities, also in the form of anti-democratic practices'. George Papademetriou (2023: 199) noted that the Israeli private surveillance software firm NSO Group's pivot in the early 2010s to marketing its products to governments rather than private entities 'proved highly lucrative', illustrating how illiberal politics can serve the profit-seeking goals of private firms. In China, Jingyang Huang and Kellee Tsai (2022: 26) found that 'the state learned to co-opt and cooperate with a private surveillance industry … [creating] dynamics of state–capital relations as mutually vested in preserving regime durability'. Indeed, it was clear that a confluence of interests was emerging between global technology firms and authoritarian states, although the impact of these relationships on authoritarianism was yet to be examined.

This article contributes to this final fledgling field of research on the political economy of digital authoritarianism, bringing lessons from broader scholarship on digital authoritarianism and the foreign relationships of authoritarian regimes in order to understand the significance and impacts of the links between foreign private

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

technology companies and authoritarian resilience. It uses evidence from Iran to interrogate the phenomenon. Iran is an 'extreme case' that is an ideal site through which to observe this phenomenon because it features on almost every index as one of the least free and most technologically advanced states on earth.[1] Despite the international sanctions environment, the Iranian regime bears a resemblance to most other technologically advanced authoritarian states in that it relies heavily on foreign technology to meet its technological innovation needs. This has led to the development of myriad relationships with the private global technology sector and makes Iran an excellent site from which to examine the link between the foreign technology trade and digital authoritarianism. The article examines three key case studies of foreign technology companies that have operated in Iran over the past two decades.

The study unfolds across three sections. The first interrogates the concept of authoritarian resilience and identifies points in which scholarship on digital authoritarianism, the international relations of authoritarian regimes and authoritarian economics intersect on the phenomenon. It then proposes four mechanisms through which the global technology trade can contribute to authoritarian resilience. The second section explains case selection and provides a background on the Iranian technology landscape. The final section undertakes empirical analysis to test the four mechanisms in order to understand how relationships with technology companies have supported the Iranian regime's deployment of technology in service of its survival goals. The article argues that while global technology companies lack the ideological or geopolitical interests that drive the engagement between authoritarian regimes and other foreign actors, digital authoritarianism has fomented the emergence of an intense overlap in interests between foreign commercial goals and authoritarian survival goals. In practice, this means that foreign technology companies have a similar impact to that of the many other actors that interact with authoritarian regimes, contributing to authoritarian resilience and survival, even if often inadvertently or indirectly.

The findings further current debates on digital authoritarianism, bridging the gap between the political economy of authoritarianism and the international aspects of authoritarian regimes to draw attention to the ways that the interests of the global technology sector are aligning with – and fortifying – the survival-seeking goals of authoritarian regimes. Empirically, the findings also highlight the important role that the global technology sector as a whole is playing in digital authoritarianism and the rapid technological advance of authoritarian regimes. While the surveillance technology trade has to date understandably received the most significant attention, the sector as a whole is contributing significantly to digital authoritarian ambitions and, as a by-product, to authoritarian resilience.

Connecting the dots between digital authoritarianism, the foreign technology trade and authoritarian resilience

Survival is the primary goal of every authoritarian regime (Frantz 2024), and as a result it remains an area of significant scholarly focus. An authoritarian regime's chances of survival depend on its ability to develop and maintain resilience against internal and external threats. This is based on a strategic toolbox that has been

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

conceptualized in various ways. To Johannes Gerschewski (2013), authoritarian stabilization and resilience requires a combination of legitimation, co-optation and coercive strategies. To Daniel Treisman and Sergei Guriev (2015), regime resilience is built from co-optation, censorship, propaganda and repressive measures. To Oliver Schlumberger et al. (2024), stability and control boil down to autocrats: (1) knowing their populations, potential threats and grievances and how to maintain control, (2) being able to influence the *behaviour* of citizens and (3) being able to influence the *beliefs* of their population. While it is beyond the scope of this article to contribute further to these largely uncontroversial (and often overlapping) models, it notes that all authoritarian regimes draw on a range of strategies to proactively maintain control and promote regime resilience (Morgenbesser 2020).

The literatures on digital authoritarianism, the international relations of authoritarian regimes and authoritarian economics intersect in four prominent ways in relation to regime resilience-building. First, all three literatures recognize the importance of regime efforts to foment a veneer of competence and progress. These efforts generate political capital by creating a sense that daily life is improving under skilful regime governance. For example, regimes might implement economic policies that support long-term economic growth in order to distribute wealth, and therefore generate support for the regime (Hankla and Kuthy 2013). The same goal often drives the completion of major development projects (Rodan and Jayasuriya 2009), the provision of jobs and other subsidies that contribute to the regime–population social contract (Conduit 2017), and efficient and effective service delivery (Cassani 2017). Indeed, Guriev and Treisman (2019: 101) noted that contemporary autocrats prefer to use a 'rhetoric of economic performance and provision of public services that resembles that of democratic leaders far more than it does the discourse of threats and fear embraced by old-style dictators'. In this regard, the literatures intersect prominently in relation to *building political capital through enhanced service delivery*. A broad range of pre-digital era social services have been linked to authoritarian resilience agendas, including healthcare service provision (Duckett and Munro 2022) and the delivery of basic infrastructure such as clean water (Brinkerhoff et al. 2012). International actors can contribute to this process by providing economic aid that enables a regime to better provide for its populations (Hagmann and Reyntjens 2016; von Billerbeck and Tansey 2019), while technology can enhance service delivery through network hardware that increases broadband or mobile telecommunications access for citizens, or software that helps streamline the delivery of government services through e-governance portals (Maerz 2016). The associated enhancement in state technological capacity can meaningfully improve citizens' social and economic opportunities, while also fostering development. This can generate popular legitimacy (even if only in a temporary or contingent manner (Brinkerhoff et al. 2012)), representing an important contribution to regime resilience.

The second point of intersection is a flow-on effect of increased regime governance capacity: *an enhanced capacity to repress*. This may not be an outcome that international backers intend (Tansey 2016) but can be a by-product of other efforts. As Sarah von Billerbeck and Oisin Tansey (2019: 703) noted:

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

> While [international] capacity-building efforts often aim to promote democratic governance, they can contribute to authoritarian outcomes when elites use the state's new-found powers to pursue repressive policies … Manipulating elections requires administrative capacity and technical knowledge. Repressing rival elites and constraining the citizenry requires state institutions that have the capacity to monitor and control, often through coercion.

Digital authoritarianism can contribute to regime resilience through similar dynamics. For example, modernized network infrastructure can enhance a regime's capacity to monitor citizens' technology use, opening the door for more sophisticated forms of repression. Many such technologies have the added benefit of being protected by a veneer of legitimate use, enabling technology companies and their regime clients to leverage the language of development and progress to procure products that are simultaneously deployed to repress.

The third intersection in the three literatures takes place in relation to the *provision of material resources that can be used to buy off elites or would-be opponents*. Authoritarian economics and international relationships can support the co-optation of would-be opponents by offering political or material inducements that incentivize loyalty. This includes distributing lucrative state contracts (Baczko et al. 2018), strategically privatizing state-owned assets, including technology infrastructure, into the hands of loyalists (Pfeifer 2016), giving preferential access to telecommunications operating licences or business subsidies, distributing scholarships for foreign study and welfare payments (Dalmasso 2018; Del Sordi 2018; Escribà-Folch 2012), appointing such individuals to prestigious state posts (Schatz 2009) or co-opting them into legislatures or other elected bodies (Frantz and Kendall-Taylor 2014). International actors can enhance these dynamics: Andrey Tomashevskiy (2017: 421) found that 'investors send larger FDI amounts to states where ex ante coup risk is high to enhance the effectiveness of a dictator's patronage strategy', whereas Jakob Tolstrup (2015: 674) noted that foreign states can provide financial resources to support vote-buying during elections. International business engagement in authoritarian regimes is often guided by myriad legal arrangements to support this dynamic. In states such as Syria, for example, foreign companies are legally required to appoint local shareholders, who are usually members of the ruling elite (Baczko et al. 2018).

The final point of intersection in the three literatures relates to the *sale of technology explicitly designed for repression*. Scholars of the international relations of authoritarian regimes have long noted the key role that foreign states have played in supporting repression, which can include providing the military hardware needed to control and repress a population, or direct involvement in repression (Tansey 2016). This includes the provision of essential military aid during crises, such as the 2011 Saudi-led mobilization of Gulf Cooperation Council armies to assist the Bahraini regime to quell popular unrest (Tansey 2016) or the Myanmar junta's ongoing purchase of weapons parts from states and private corporations to facilitate its brutal repression (Hatton 2023). Private companies within authoritarian states are also involved in the provision of material support for repression. This includes the Wagner Group in Russia, which has engaged on a for-profit basis to actively support Russia's crackdowns at home and abroad. Similarly,

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

the Iranian regime claims that more than 5,000 private companies are involved in its domestic arms manufacturing sector (Boussel 2023). Technology too can make a significant contribution to a state's repressive apparatus, as seen in the commercial–state surveillance complex that Liu (2019) noted in China.

This article proposes that these four themes that exist at the intersections of the literatures on digital authoritarianism, the international relationships of authoritarian regimes and authoritarian economics, also act as mechanisms through which the interests and actions of the global technology sector interact with – and enhance – regime resilience agendas. The final part of this section explains how these mechanisms work through reference to already known examples of foreign technology sales in authoritarian states, before undertaking an in-depth examination of Iran in the following section in order to understand the full scope and impact of the mechanisms on authoritarian resilience.

The four mechanisms and the global technology market

Resilience mechanism 1: Building political capital through enhanced service delivery

Foreign technology companies can augment regime service delivery, contributing to a sense of regime competence and state modernization (Kabanov 2020). Examples include Huawei's 'safe cities' surveillance technology that the company markets as a tool for enhancing citizen safety and law-and-order (Zhihui 2016), Ericsson's collaboration with Orange Egypt to upgrade Egypt's network architecture, and the work of foreign technology consulting firms such as AtkinsRéalis that are being paid to deliver the Saudi Crown Prince Mohammad bin Salman's pet project, the futuristic NEOM city (Uddin 2022). All such relationships are playing a significant role in filling domestic technology gaps and supporting regime development and progress agendas. They may therefore contribute to authoritarian resilience.

Resilience mechanism 2: Increasing a regime's capacity to use legitimate technology for repression

Foreign technology companies are playing a visible role in the distribution of tools that either incidentally strengthen a regime's ability to repress or have clear 'dual use' potential. Examples include IBM's efforts to provide data-mining expertise to reduce traffic congestion in China, that as a by-product can theoretically also serve as a powerful surveillance tool (Greenberg 2009). Another example is Huawei's 'safe cities' technology noted above, which has been purchased by both authoritarian and democratic states but has surveillance and data-gathering capacities that are vulnerable to misuse (Hillman and McCalpin 2019). In fact, most foreign firms maintain that their products have legitimate uses. This even includes the NSO Group, whose Pegasus surveillanceware has been used by more than a dozen authoritarian regimes to track journalists, activists and opponents (Benjakob 2022). Its mission statement is 'We work to save lives and create a better, safer world' (NSO Group 2024).

Resilience mechanism 3: Providing a regime with material resources that can be used to buy off elites or would-be opponents

The global technology trade is well placed to provide authoritarian regimes with material inducements to 'buy' a support base (Wintrobe 1998). While some

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

international technology is sold directly to a regime, foreign firms are often forced to engage with local elites via franchises or conglomerates. Syria's first cellular network provider, Syriatel, is an example of this, as it was co-owned by the Egyptian telecommunications firm Orascom and Rami Makhlouf, the first cousin of the Syrian president. These international arrangements provide significant opportunities for regimes to distribute lucrative technology contracts to supporters in reward for loyalty, enhancing their stake in the regime's survival and therein contributing to regime resilience.

Resilience mechanism 4: Selling technology explicitly designed for repression

Finally, the global technology trade can contribute to digital authoritarianism and authoritarian resilience by directly increasing a regime's capacity to repress. Foreign technology companies around the world produce hardware and software that has been purchased by authoritarian regimes with the sole purpose of enhancing their repressive apparatus. This includes companies such as the NSO Group or Hacking Team, which have sold military-grade spyware that has been deployed against dissidents, and a leaked Cisco sales presentation that proposed hardware for China's Great Firewall (Stirland 2008). Such technologies can be leveraged to provide the backbone of digital authoritarianism and are endowing regimes with an extensive and unprecedented opportunity to enhance regime resilience.

Scope conditions and limitations

Before proceeding to the Iran case study, it is important to acknowledge the scope both of the four mechanisms, and specifically of this article. First, the mechanisms have been designed to answer a question about the resilience of authoritarian regimes, but may also be relevant to state capacity-strengthening in other contexts, including states experiencing democratic backsliding. However, given the research question and the newness of the mechanisms, this article focuses only on authoritarian states. Second, while each of the four mechanisms is readily distinguishable, the human-mediated nature of regime–foreign technology firm relationships and the often-multiple applications of individual technology products means that the mechanisms may overlap. Third, almost all authoritarian regimes rely on some level of repression to survive, while states at war still need to deploy 'soft' tools to maintain a support base. Individual mechanisms may nonetheless be more or less prominent in certain contexts. In times of peace and stability, for example, regimes may have the strategic space to design policy interventions that broaden their support base or enhance their popular legitimacy. This could see Mechanisms 1 or 3 take on particular prominence, with foreign relationships being leveraged to source technology that enhances governance or offers additional opportunities to strengthen the regime's social contract or ruling coalition. By contrast, Mechanisms 2 and 4 may be more prominent during popular protests, intra-regime instability or war, when regimes lean more heavily on foreign companies to fund or supply their repressive apparatuses. Finally, the diversity among authoritarian states also means that the mechanisms will likely be deployed in varying configurations in different jurisdictions. In this way, while it is expected that the four mechanisms apply to some extent in all authoritarian contexts, they are more of a 'menu' (Morgenbesser 2020) than an exact prescription.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Case selection

This article is based on a single case study analysis of Iran that draws from data collected from a range of primary and secondary sources in English and Persian. This includes newspaper articles, government websites, court documents, technology industry periodicals, corporate annual reports, social media accounts and Securities and Exchange Commission (SEC) filings, as well as NGO reports. Iran was chosen because it forms an 'extreme case' of digital authoritarianism, ranked in the 2022 Freedom on the Net index as having the third least-free internet ecosystem on earth (Freedom House 2023a). Jason Seawright (2016: 495) argued that extreme cases are valuable to study because they offer the 'best chances of facilitating discovery'. This discovery process is appropriate given the contemporaneous nature of the phenomenon: as noted above, the political economy of digital authoritarianism has only begun to attract significant scholarly attention. The international sanctions regime should have acted as a barrier to foreign technology procurement, but the Iranian regime has successfully pursued relationships with technology companies from across almost every continent. In fact, the sanctions regime has acted to cast rare light on the usually opaque relationships between the global technology sector and authoritarian regimes via court or government processes, which means that Iran's foreign technology relationships are better documented and more certain than those of many other authoritarian states.

Iran is an instructive case to observe because, while China has become the archetypal case of digital authoritarianism broadly (Ceci and Rubin 2022; Khalil 2020; Lilkov 2020; Ming-Tak Chew and Wang 2021; Taylor 2022; Wang 2021) and regime–private technology company relations more specifically (Huang and Tsai 2022; Liu 2019), the extreme level of control that the Chinese state has achieved – and the enormous domestic technology sector that supports it – make it unique. It is hard to see any other state fully replicating the Chinese model (Pan 2017), which limits its comparative value. By contrast Iran more closely resembles the second tier of highly ambitious and advanced 'extreme' digital authoritarian states such as Russia, Venezuela, Myanmar and Saudi Arabia, which all depend on the international technology sector. This case study therefore represents an opportunity to understand the role being played by the global technology trade in a large number of other 'like' extreme states.

The article focuses on three foreign technology companies that have undertaken substantial business in Iran: the South African telecommunications provider MTN, the German/Finnish joint venture Nokia Siemens Networks (now known as Nokia Networks) and the Chinese surveillance technology giant Tiandy. Although Iran has relationships with tens of foreign technology companies, these three have been involved in Iran since the early 2000s and remain active in the country today. Each has faced scrutiny as a result of foreign court challenges and sanctions proscriptions, providing the level of case certainty required to analyse the article's four mechanisms. Given the long tenure of each company's engagement in Iran, they also offer an opportunity to observe the potential impacts of engagement across periods of regime strength and weakness, including during crises.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Background: The Islamic Republic of Iran

The Iranian regime came to power after the tumultuous 1979 Iranian Revolution, forming a hybrid authoritarian state in which power is unevenly distributed between the country's theocrats and elected officials (Ghobadzadeh and Rahim 2016). Although the country conducts somewhat competitive (although not free) elections that facilitate a modicum of democratic alternance, elected officials such as the president and members of parliament are frequently sidelined by the theocratic elements of the state, including Supreme Leader Ali Khamenei and para-state institutions such as the Islamic Revolutionary Guards Corps (IRGC) (Ansari 2014). The IRGC, which is close to the supreme leader, has its own military and security apparatuses that operate in parallel with – and often undermine – the formal institutions of the state, making Iran one of the least free states on earth.

The Iranian regime is among the world's most sophisticated practitioners of digital authoritarianism on the basis of its ongoing (although not yet complete) efforts to establish a domestic internet ecosystem akin to China's Great Firewall or North Korea's Kwangmyong, its hacking of opponents, online disinformation operations and use of smart surveillance technology (Conduit 2022). Although Iran has an advanced domestic technology industry, the country is not technologically self-sufficient, which leaves it reliant on foreign hardware, software and services to fill domestic technology gaps. Iran's international technology trade is driven by two distinct but often overlapping needs, which makes Mechanism 2 particularly prominent in the analysis below. The first is the legitimate technology requirement of its large population and economy, which has led to the establishment of commercial relationships that provide technology to facilitate the country's access to the internet or software that supports healthcare and other critical industries. The second and more malevolent aspect of Iranian technology procurement is driven by the regime's resilience goals (Michaelsen 2018). The latter has seen the regimes and entities linked to it, including the IRGC, the Ministry of Defence and policing bodies, develop relationships with foreign surveillance and technology companies to build regime resilience. The IRGC and supreme leader also exercise influence through an extensive but shadowy network of business interests across the economy (Azadi 2019). The blurred lines between the state, para-state and shadowy enterprises linked to the regime's elite mean that the international technology trade is conducted with a range of entities and often through opaque franchises.

The Iranian regime and the private technology trade: Three case studies

MTN Group

The South African telecommunications giant MTN Group has conducted business in Iran since the mid 2000s after the Iranian regime announced that it would license a second cellular network operator in order to further the country's development. The then-minister of communications and information technology, Ahmad Motamedi, explained that a second operator was needed to overcome the underdevelopment of Iran's telecommunications infrastructure, which he estimated had led to rates of cell phone uptake that lagged 10 years behind the global baseline (Islamic Republic News Agency 2004). MTN won the licence for the new operator under an agreement in which it would work with a quasi-regime conglomerate

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

made up of the defence ministry subsidiary Iran Electronics Industries and the US-sanctioned Bonyad Mostazafan. Bonyad Mostazafan is an organization led by former IRGC commander and former defence minister Hossein Dehghan and is described by the US Department of the Treasury as 'a key patronage network for the Supreme Leader of Iran' (US Department of the Treasury 2023). MTN owns a 49% stake in what became MTN IranCell, purportedly acting as its 'technical implementation partner' (Access Now 2012).

MTN IranCell began operations in 2006. Its lower pricing and the ease of buying its sim cards made the company a welcome addition to the Iranian telecommunications market, which had long been held back by the red tape and inefficiency of the state-owned operator MCI Hamrah-e Avval. The new network also contributed significantly to the country's technological advancement. With its launch, MTN IranCell brought MMS picture messaging to Iran for the first time, and in 2015 it launched Iran's first 4G cellular network. In 2022, MTN reported that it had invested more than US$10 billion in IranCell since winning the licence (TeleGeography 2023).

MTN's presence in Iran first attracted controversy during the Green Movement uprising that was spurred by Iran's disputed 2009 presidential election, which at the time was the worst crisis that the regime had faced in its 30-year history. The group's operational role in MTN IranCell raised questions as to the role that it played in assisting the regime's resilience-building measures during the crisis, which included significant disruptions to the mobile network. Alongside the enforcement of a 40-day SMS blackout (Radio Zamaneh 2009), the regime implemented widespread cell phone surveillance (Freedom House 2011).

Given that these interruptions took place across all networks, including MTN Irancell, questions were raised as to whether the South African company was involved in user surveillance, and consented to or implemented the 40-day SMS blackouts on its network that had been ordered by the minister of intelligence (Radio Zamaneh 2009). Contrary to widespread reports that SMS was not working on its network, MTN's executive director, Nozipho January-Bardill, claimed that the 'MTN network is running in Iran and there is nothing wrong with it' (Reuters 2009). MTN IranCell did, however, concede in August that further network interruptions were taking place. Days before the expected escalation of protests targeting President Mahmoud Ahmadinejad's disputed inauguration, MTN IranCell alerted customers that its network would experience three days of vague 'technical' problems (Daragahi 2009). In addition, the lawful interception system sold by Nokia Siemens (discussed below) was installed on the MTN IranCell network, and may have been used to surveil customers.

Despite the significant disruptions to its ability to provide service, 2009 nonetheless proved a profitable year for the company, with MTN's annual financial report declaring a 35% revenue increase from IranCell. In the context of a massive regime crackdown, IranCell attracted an additional 7 million subscribers, increasing its market share to 40% (MTN Group Limited 2010: 14) and reflecting O'Donnell's (1978) decades-old observation that regime and commercial interests often coalesce to deliver benefits to both parties. Significant international scrutiny after 2009 failed to deter MTN's expansion of operations in Iran. It subsequently signed an agreement to invest $295 million for a 49% stake in the Iranian broadband network

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Iranian Net (Reuters 2017) and $22 million in the Iranian ridesharing and food delivery app Snapp. Snapp has been widely criticized for violating user privacy (Shahrabi 2017), enforcing the country's hijab mandates inside their cars (Esfandiari 2019), and for allegedly sharing user location data with authorities during the 2022–2023 protests (Fertoli and Vargas 2023).

Although there is no evidence that MTN intended to contribute to regime resilience during the 2009 crisis or subsequently, several of this article's proposed mechanisms are nonetheless apparent in its engagement in Iran (Table 1). In this case, a overlap between MTN's narrow corporate interests and the regime's developmental technology agenda led to the formation of an enduring relationship between an international technology corporation and a conglomerate made up of a regime subsidiary and its elite. MTN had a significant service-delivery impact from the moment it entered Iran, giving Iranian consumers choice, price competition and less red tape than its state-owned competitor, and delivering political capital to the regime (Mechanism 1). It also supported the advancement of Iran's telecommunications infrastructure by introducing new technology, including next-generation mobile frequencies. This directly complemented and contributed to the regime's development and modernization agenda, and may therefore have enhanced regime resilience. But any increase in technological capacity and resources in an authoritarian regime comes with significant risk: with MTN providing technical implementation services that ensured the reliable operation of Iran's second-largest network, the regime was able to use the network to implement its own separate surveillance agenda during the 2009 crackdown (Mechanism 2), including SMS shutdowns and surveillance of cell phone users. MTN's partnership with Bonyad Mostazafan and Iran Electronics Industries, two entities linked to the regime and its elite, including the IRGC, epitomized Mechanism 3, highlighting the co-optive value of the international technology trade by distributing the spoils of a lucrative international partnership to regime elites whose compliance was essential to regime survival. This echoed long-observed patterns of both authoritarian economics (Baczko et al. 2018) and the international relationships of authoritarian states (Tansey 2016; Tolstrup 2015).

In this regard, while MTN may not have actively sought to contribute to regime resilience, it has provided services and expertise over the course of nearly three

Table 1. Presence of the Four Mechanisms

	MTN	Nokia Siemens	Tiandy
Mechanism 1: Building political capital through enhanced service delivery	Y	Y	Y
Mechanism 2: Increasing a regime's capacity to use legitimate technology for repression	Y	Y	Y
Mechanism 3: Providing a regime with material resources that can be used to buy off elites or would-be opponents	Y		Y
Mechanism 4: Selling technology explicitly designed for repression			Y

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

decades that triggered three of the four resilience mechanisms. This underlines the complex interaction between the foreign technology trade and digital authoritarianism, because while MTN had no evident ideological stake in the regime, the overlap between its commercial interests and the regime's survival interests led to the emergence of a narrow but enduring crossover in interests that has proven mutually beneficial.

Nokia Siemens Networks/Nokia Networks

The deployment of Nokia Siemens Networks (now Nokia Networks) technology on the two main Iranian cellular networks also drew attention during the 2009 protests. The previous year, Nokia Siemens had sold its 'lawful interception technology' to MTN IranCell, and lawful interception technology and a monitoring centre to the state-owned MCI Hamrah-e Avval. The products provided the two telecommunications companies with the ability to monitor, listen and track fixed-line and mobile calls, a technology that is used worldwide for legitimate law enforcement purposes but has potential secondary malevolent uses.

Nokia Siemens' lawful interception technology further underlined the interplay between Mechanisms 1 and 2 (Table 1). Legal monitoring technology may have assisted the Iranian authorities in legitimate law-and-order activities, furthering the regime's ability to govern, and offering stability and safety to its citizens, thereby delivering a political capital dividend to the regime (Mechanism 1). However, the regime's dual use of the technology quickly became apparent. Similar to the adverse impacts of legitimate peacebuilding initiatives that von Billerbeck and Tansey (2019) noted, activists detained during the 2009 protests reported that interrogators had presented them with printed transcripts of telephone conversations that were acquired using the kind of legal technology that Nokia Siemens had sold, highlighting that the regime's enhanced policing capacity was also enhancing its capacity for repression (Mechanism 2).

The company, which is now known as Nokia Networks, subsequently expanded its operations in Iran. In 2016, it signed an agreement with an Iranian internet service provider to introduce high-speed wireless TD-LTE technology (Mechanism 1). The signing ceremony was attended by the Iranian communications minister (Fars News 2016), which underlined the company's importance to the Iranian regime. In a 2020 filing to the US Securities and Exchange Commission, Nokia Networks reported that in the previous year, it had provided: 'limited local delivery of radio, core and transmission equipment, including associated services, to MTN Irancell and some software and features to Mobile Communications Company of Iran (MCCI). We also provided some services to local fixed networks operators, [including the] Telecommunication Company of Iran (TCI)' (Nokia Corporation 2020). By 2023 the company reported that its sales to MTN made up 99% of its business in Iran, and that it was no longer taking on new business in the country (Nokia 2023).

Nokia Siemens/Nokia Networks' work in Iran sheds light on how the interests of foreign technology companies and authoritarian regimes can coalesce. It has repeatedly invoked the legitimate applications of their products to justify continued sales, underlining that legal monitoring technology is used by law-enforcement agencies globally. In the wake of the 2009 protests, it issued a statement in which

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

it underlined that 'It is unrealistic to demand … that wireless communications systems based on global technology standards be sold without that capability' (Nokia Siemens Networks 2010). A Nokia Siemens spokesperson later cited an acknowledgement by the UN's International Telecommunications Union (ITU) that legal communications monitoring is a right of all states (Free Speech Debate 2012).

The company does, however, acknowledge the complexity of its business in Iran. Its annual reports frequently include a disclaimer along the lines of, 'although it is difficult to evaluate with any reasonable degree of certainty, we have concluded that we cannot exclude the possibility that [our partners are] … owned or controlled, directly or indirectly, by the government of Iran'.[2] But this uncertainty and ethical complexity does not appear to concern the company. Following the company's embroilment in the 2009 crackdown Nokia Siemens spokesman Ben Roome had explained that foreign companies should not have to consider the potential end-uses of the technology they sell: 'Technology providers just provide what countries and states require them to provide. They have been in the habit of not making a judgement call on how that technology may be used or what the end result of that use may be … We're not in the business of deciding what laws should exist in a particular country' (Free Speech Debate 2012). Indeed, it was clear that Nokia Siemens was determined to depict its engagement in Iran as value-neutral, enabling the expansion of the mutually beneficial relationship between a profit-hungry private technology company and a technology-hungry regime (Mechanism 2), that the regime leveraged to enhance its own chances of survival.

Tiandy Technologies

Tiandy is one of the world's largest manufacturers of video surveillance technology. The Chinese firm, which has operated in Iran since 2007 (Tehran Bureau 2022), has developed commercial relations with the regime and its para-state organizations, including the IRGC. The Tiandy Iran website listed the above-mentioned supreme leader and IRGC-linked Bonyad Mostazafan and a government prison labour organization among its customer base (Tiandy Iran 2021). Tiandy surveillance cameras are used by the defence ministry subsidiary Iran Electronics Industries, also noted above. Tiandy has sold network video recording technology and video surveillance cameras to the Iranian military. Its surveillance cameras have been documented providing perimeter security around military bases (IVPM 2021). In late 2022, the US accused Tiandy of evading sanctions by enabling 'the procurement of U.S.-origin items for use by the Islamic Revolutionary Guard Corps' (US Department of Commerce 2022). Unlike MTN or Nokia Siemens, Tiandy indirectly sells its products via local distributors, including Radis Vira Tejarat (Mechanism 3).

A harsh spotlight fell on Tiandy during the 2022–2023 protests that began in September 2022 after a 22-year-old Kurdish-Iranian woman, Mahsa 'Jina' Amini, died in the custody of Iran's morality police. Amini had been arrested for improperly wearing her hijab, the mandatory head covering that women in Iran are forced to wear in public. Her death caused public outcry, with protesters across the country chanting 'Women, Life, Freedom' and 'Death to the Dictator' in the streets (Hafezi 2022), leading to what the IRGC chief described as 'the most dangerous and powerful riot' in the regime's history (Khabar Online 2023). The regime's

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

subsequent technology-fuelled crackdown led to particular scrutiny of its imported smart surveillance cameras, which the head of the parliamentary legal and judicial committee, Mousa Ghazanfarabadi, explained reduced 'the presence of the police, as a result of which there will be no more clashes between the police and citizens' (Enghlab Islami News Agency 2022). This made smart surveillance cameras a particularly powerful tool in the regime's survival toolkit.

Tiandy's sales of surveillance cameras to Iran had purportedly doubled in the year of the Mahsa Amini protests (Faucon and Lin 2023), and its equipment emerged as significant in the crackdown. In 2023, the EU imposed sanctions on Tiandy's local distributor Radis Vira Tejarat, which the EU identified as 'the Iranian representative of the company Tiandy Technologies' (European Union 2023). The company was sanctioned on the basis that, 'During the protests following the death of Mahsa Amini in police custody in mid-September 2022, its equipment has been used by the Iranian security forces, including the Islamic Revolutionary Guard Corps (IRGC), its Basij and the Law Enforcement Forces of the Islamic Republic of Iran (LEF), to brutally suppress the nationwide protests' (European Union 2023: 16).

Indeed, of all three companies, Tiandy's engagement was most overtly linked to the regime's resilience agenda, given that its customers have included the most sensitive organs of the Iranian state such as the IRGC (Table 1). Its dual-use products were used for both mundane purposes such as military base security (Mechanism 1) and more repressive uses (Mechanism 2). According to the EU, Tiandy products were directly deployed to support the regime crackdown (Mechanism 4). In this regard, Tiandy's interaction and impacts in Iran bore remarkable resemblance to the foreign states that have actively supported repressive agendas on the basis of ideological rather than commercial interests (Tansey 2016). This interaction is substantial and significant, because as Ghazanfarabadi's comments underlined, such technology directly reduces the risk of conflagrations between the regime and its citizens. This ensured that a foreign technology company had become a key enabler in the regime's drive to enhance regime and control.

Conclusion

This article asked how the sales of foreign technology interact with authoritarian regime resilience agendas. Proposing four mechanisms through which such a process takes place, it argued that commercial and authoritarian agendas have frequently found an opportunistic overlap that has seen foreign technology directly deployed in the service of digital authoritarianism and authoritarian resilience. Today Iran stands as one of the most digitally sophisticated authoritarian regimes on the planet, even though the country is not technologically self-sufficient. Indeed, foreign technology companies have played a key enabling role in the Iranian regime's pursuit of its digital authoritarian ambitions. Although recent work has argued that authoritarian states look to Chinese companies for internal security (or resilience) solutions, and the US to shore up external security (Chestnut Greitens and Kardon 2024), this article noted no distinction in Iran's choice of which global companies with whom to collaborate. Foreign technology companies from across the globe provided Iran with wares and services ranging from mundane

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

network hardware to powerful video surveillance technology, all of which had the potential to be leveraged by the regime in pursuit of its own survival.

Indeed, the Iran case illustrated interactions between the foreign technology trade and authoritarian resilience across all four mechanisms. First, the international technology trade contributed to regime resilience by increasing the Iranian regime's ability to deliver essential services such as cellular networks and law and order, thereby enhancing its popular legitimacy. This was most evident in MTN's long engagement in the country via MTN IranCell, which has supported the regime's development agenda by enabling the operation of a second cell phone provider, introducing lower prices, less bureaucracy, and becoming a key player in the modernization of the country's lagging cell phone infrastructure. Just over a decade after MTN entered Iran, the country would have cell phone penetration levels comparable to advanced economies in the region such as Israel (GSMA 2019). This progress delivered political capital dividends to the regime.

The second way that the international technology trade interacted with the regime's resilience agenda relates to the first mechanism: enhancing a regime's general technological capacity can unintentionally increase that regime's ability to leverage legitimate technology for repression. This was the case in relation to both MTN and Nokia Siemens. Both companies provided legitimate services and technology that aimed to increase Iran's basic technological capacity, which the regime then redirected to repress its population during the 2009 crackdown. The veneer of legitimate use associated with the sale of mundane products has meant that even though both companies faced significant criticism for their product sales after 2009, both companies remain active in Iran today.

Third, Iran's foreign technology trade interacted directly with the regime's co-optation agenda. Much international trade is conducted with regime-adjacent entities and members of its elite, including MTN's long-term partnership with a conglomerate linked to Bonyad Mostazafan and the defence ministry. These are lucrative arrangements that enable the regime to distribute the financial spoils of international technology procurement among officials and regime-loyal entities. Such financial arrangements have long been known to increase those entities' stake in regime survival.

The fourth way that the international technology trade interacts with digital authoritarianism in Iran is by selling technology explicitly designed for repression. This was particularly evident in the surveillance technology that Tiandy sold in Iran in the lead-up to – and during – the 2022–2023 protests that led to its local distributor being sanctioned by the EU for its complicity in the crackdown, and to Tiandy being directly sanctioned by the US for selling products to the IRGC. Its sale of smart surveillance cameras highlighted the key role that foreign technology companies were playing in providing technology that directly replaced humans in the state's repressive apparatus. Such technology is becoming a powerful regime resilience tool because it offers population control solutions without the risk of in-person conflagrations.

Iran may be an 'extreme case' of these dynamics, but there is much reason to expect that the four mechanisms could be replicated across many other authoritarian jurisdictions. These findings therefore have implications for both the understanding of the international relations of authoritarian regimes and for digital

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

authoritarianism. First, they highlight that scholars looking at the international relations of authoritarian regimes must also pay attention to regimes' foreign business partners who can inadvertently provide material support for authoritarian agendas. This is significant because it highlights that the international technology trade is facilitating authoritarian resilience in a similar fashion to previously observed ideologically or geopolitically driven actors such as states or regional organizations. Indeed, while the relationships between authoritarian regimes and global technology companies almost always reflect transactional overlap rather than a full meeting of minds, all three Iranian cases revealed an intense and enduring interaction that directly supported the regime's resilience agenda. This also raises questions about whether global technology sales could impact state capacity and digital authoritarian 'practices' in non-authoritarian jurisdictions, which is a question beyond the scope of this article that must be taken up by future researchers.

Second, the findings have implications for the study of digital authoritarianism, which to date has paid extensive attention to how state-to-state relations have led to the diffusion of technology, but are yet to explore fully the political economy of the phenomenon and the role played by the international private technology sector. Indeed, in many ways, foreign technology companies are providing the backbone of digital authoritarianism in non-technological self-sufficient authoritarian states, making the global private technology sector a central player in contemporary autocrats' efforts to achieve regime resilience.

Acknowledgements. The author would like to thank Dr Neda Zeyghami for her invaluable research assistance on the article, as well as the anonymous peer reviewers whose detailed and thoughtful feedback contributed significantly to the final version of this article.

Financial support. This work was supported by an Australian Research Council DECRA fellowship DE220100622.

Notes

1 See, for example, Freedom House (2023a, 2023b).
2 See, for example, Nokia Corporation (2020, 2023).

References

Access Now (2012) MTN must stand up for its users, meet international obligations. Access Now, press release, November, https://www.accessnow.org/wp-content/uploads/archive/docs/IranCell%20MTN.pdf.

Ansari A (2014) *Iran: A Very Short Introduction*. Oxford: Oxford University Press.

Azadi P (2019) *Governance and Development in Iran, Stanford Iran 2040 Project*. Stanford: Stanford University.

Baczko A, Quesnay A and Dorronsoro G (2018) *Civil War in Syria: Mobilization and Competing Social Orders, Problems of International Politics*. Cambridge: Cambridge University Press.

Baser B and Ozturk AE (2020) Positive and Negative Diaspora Governance in Context: From Public Diplomacy to Transnational Authoritarianism. *Middle East Critique* **29**(3), 319–334. https://doi.org/10.1080/19436149.2020.1770449.

Benjakob O (2022) The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware, 2022. *Haaretz*, 5 April, https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000.

Boussel P (2023) Will Iran supply the world with low-cost weapons? *GIS Reports Online*, 9 January, https://www.gisreportsonline.com/r/iran-weapons/.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Brinkerhoff DW, Wetterberg A and Dunn S (2012) Service Delivery and Legitimacy in Fragile and Conflict-Affected States: Evidence from Water Services in Iraq. *Public Management Review* **14**(2), 273–293. https://doi.org/10.1080/14719037.2012.657958.

Cassani A (2017) Social Services to Claim Legitimacy: Comparing Autocracies' Performance. *Contemporary Politics* **23**(3), 348–368. https://doi.org/10.1080/13569775.2017.1304321.

Cebul M and Pinckney J (2021) *Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution*. United States Institute for Peace Special Report 499. Washington, DC: United States Institute of Peace.

Ceci MV and Rubin L (2022) China's 5G Networks: A Tool for Advancing Digital Authoritarianism Abroad? *Orbis* **66**(2), 270–288. https://doi.org/10.1016/j.orbis.2022.02.013.

Chestnut Greitens S and Kardon I (2024) Playing Both Sides of the U.S.–Chinese Rivalry. *Foreign Affairs*, 15 March, https://www.foreignaffairs.com/united-states/playing-both-sides-us-chinese-rivalry.

Codreanu CM (2022) Using and Exporting Digital Authoritarianism: Challenging Both Cyberspace and Democracies. *Europolity: Continuity & Change in European Governance* **16**, 39–65.

Conduit D (2017) The Patterns of Syrian Uprising: Comparing Hama in 1980–1982 and Homs in 2011. *British Journal of Middle Eastern Studies* **44**(1), 73–87. https://doi.org/10.1080/13530194.2016.1182421.

Conduit D (2022) Securing Iran in the Internet Age. In Clarke M, Henschke A, Sussex M and Legrand T (eds), *The Palgrave Handbook of National Security*. Cham: Springer International Publishing, pp. 241–260.

Cottiero C and Haggard S (2023) Stabilizing Authoritarian Rule: The Role of International Organizations. *International Studies Quarterly* **67**(2), 1–15. https://doi.org/10.1093/isq/sqad031.

Dalmasso E (2018) Between Representation and Participation: Investigating the Transnational Politics of Membership of the Kingdom of Morocco. *Political Geography* **64**, 101–103. https://doi.org/10.1016/j.polgeo.2017.07.003.

Daragahi B (2009) Iran court warns against criticizing proceedings. *Los Angeles Times*, 3 August, https://www.latimes.com/archives/la-xpm-2009-aug-03-fg-iran-trials3-story.html.

Debre MJ (2021) The Dark Side of Regionalism: How Regional Organizations Help Authoritarian Regimes to Boost Survival. *Democratization* **28**(2), 394–413. https://doi.org/10.1080/13510347.2020.1823970.

Del Sordi A (2018) Sponsoring Student Mobility for Development and Authoritarian Stability: Kazakhstan's Bolashak Programme. *Globalizations* **15**(2), 215–231. https://doi.org/10.1080/14747731.2017.1403780.

Dobson WJ (2012) *The Dictator's Learning Curve*. New York: Doubleday.

Dragu T and Lupu Y (2021) Digital Authoritarianism and the Future of Human Rights. *International Organization* **75**, 991–1017. https://doi.org/10.1017/S0020818320000624.

Duckett J and Munro N (2022) Authoritarian Regime Legitimacy and Health Care Provision: Survey Evidence from Contemporary China. *Journal of Health Politics, Policy and Law* **47**(3), 375–409. https://doi.org/10.1215/03616878-9626894.

Enghlab Islami News Agency (2022) The opponents today were once supporters of the morality police in the past [in Persian]. 24 September, https://enghelabe-eslami.com/index.php/tamas/13-khabar/siasi/48546-2022-09-24-07-32-38.html.

Erixon F and Lee-Makiyama H (2011) Digital authoritarianism: Human rights, geopolitics and commerce *ECIPE Occasional Paper 5/2011*. European Centre for International Political Economy (ECIPE), Brussels.

Escribà-Folch A (2012) Authoritarian Responses to Foreign Pressure: Spending, Repression, and Sanctions. *Comparative Political Studies* **45**(6), 683–713. https://doi.org/10.1177/00104140114278.

Esfandiari G (2019) Snapp Judgment: Iran Ride-Sharing Company at Center of 'Bad Hijab' Dispute. Radio Free Europe/Radio Liberty, 15 June, https://www.rferl.org/a/snapp-judgment-iran-ride-sharing-company-at-center-of-bad-hijab-dispute/30000859.html.

European Union (2023) Council Implementing Decision (CFSP) 2023/153. *Official Journal of the European Union* L 20 I/23. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023D0153.

Fars News (2016) Nokia Signs Contract to Launch TDD-LTE in Iran. 14 September, http://web.archive.org/web/20160914135213/http://en.farsnews.com/newstext.aspx?nn=13950624001035 (accessed 17 July 2024).

Fatafta M (2021) Transnational Digital Repression in the MENA. In Diamond L and Donahue E (eds), *Digital Activism and Authoritarian Adaptation in the Middle East*. Washington, DC: POMEPS, pp. 41–47.

Faucon B and Lin L (2023) U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup: Beijing's Exports of Video Recorders to Iran More than Doubled in 2022 as Protests Swept the Country.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Wall Street Journal, 4 February, https://www.wsj.com/articles/u-s-weighs-sanctions-for-chinese-companies-over-iran-surveillance-buildup-11675503914.

Feldstein S (2021) *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press.

Fertoli A and Vargas L (2023) Iran's Protests Morph into Quieter Rebellion. *Wall Street Journal*, 7 February, https://www.wsj.com/podcasts/whats-news/irans-protests-morph-into-quieter-rebellion/1904964a-8874-49b7-8d74-d7082ed743ee.

Foreign Affairs (2019) Does Technology Favor Tyranny? Ask the Experts, *Foreign Affairs*, 12 February, https://www.foreignaffairs.com/ask-the-experts/2019-02-12/does-technology-favor-tyranny.

Frantz E (2024) Authoritarian Survival. In Lindstaedt N and den Bosch JJJ (eds), *Research Handbook on Authoritarianism*. Cheltenham: Edward Elgar Publishing, pp. 229–243.

Frantz E and Kendall-Taylor A (2014) A Dictator's Toolkit: Understanding How Co-Optation Affects Repression in Autocracies. *Journal of Peace Research* **51**(3), 332–346. https://doi.org/10.1177/0022343313519808.

Frantz E, Kendall-Taylor A and Wright J (2020) *Digital Repression in Autocracies*. Gothenburg: V-Dem Institute.

Freedom House (2023a) *Internet Freedom Scores 2023: Freedom on the Net Report*. Washington, DC: Freedom House. https://freedomhouse.org/countries/freedom-net/scores (accessed 14 November 2023).

Freedom House (2011) *Freedom on the Net 2011: Iran*. Washington, DC: Freedom House.

Freedom House (2023b) *Freedom in the World 2023*. Washington, DC: Freedom House. https://freedomhouse.org/countries/freedom-world/scores.

Free Speech Debate (2012) Nokia Siemens' role in Iran's web spying: Interview with Ben Roome. YouTube, https://www.youtube.com/watch?v=D4KFOmmhy_A.

Gerschewski J (2013) The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes. *Democratization* **20**(1), 13–38. https://doi.org/10.1080/13510347.2013.738860.

Ghobadzadeh N and Rahim LZ (2016) Electoral Theocracy and Hybrid Sovereignty in Iran. *Contemporary Politics* **22**(4), 450–468. https://doi.org/10.1080/13569775.2016.1175097.

Gohdes AR (2020) Repression Technology: Internet Accessibility and State Violence. *American Journal of Political Science* **64**(3), 488–503. https://doi.org/10.1111/ajps.12509.

Greenberg A (2009) IBM Bets on Beijing. Forbes, 12 November, https://www.forbes.com/forbes/2009/1130/technology-china-infrastructure-pollution-ibm.html.

GSMA (2019) *The Mobile Economy: Middle East and North Africa*. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/05/ME-MENA-2019.pdf.

Guriev S and Treisman D (2019) Informational Autocrats. *Journal Economic Perspectives* **33**(4), 100–127. https://doi.org/10.1257/jep.33.4.100.

Hafezi P (2022) Iran president says Amini's death is 'tragic incident', but 'chaos' unacceptable. Reuters. 28 September, https://www.reuters.com/world/middle-east/irans-nationwide-protests-pile-pressure-state-2022-09-28/.

Hagmann T and Reyntjens F (eds) (2016) *Aid and Authoritarianism in Africa: Development without Democracy*. London: Zed Books.

Hankla CR and Kuthy D (2013) Economic Liberalism in Illiberal Regimes: Authoritarian Variation and the Political Economy of Trade. *International Studies Quarterly* **57**(3), 492–504. https://doi.org/10.1111/j.1468-2478.2012.00753.x.

Hatton C (2023) Global firms help Myanmar's military make weapons, says report. BBC News, 16 January, https://www.bbc.co.uk/news/world-asia-64250674.

Hillman JE and McCalpin M (2019) *Watching Huawei's 'Safe Cities'*. CSIS Brief, 4 November. Washington, DC: CSIS. https://www.csis.org/analysis/watching-huaweis-safe-cities.

Huang J and Tsai KS (2022) Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China. *The China Journal* **88**, 2–28. https://doi.org/10.1086/720144.

Islamic Republic News Agency (2004) Iran minister 'optimistic' about Turkish deal. BBC Monitoring Middle East. 20 December.

IVPM (2021) Tiandy's Iran Business, Sells to Revolutionary Guard and Military (Archived). http://web.archive.org/web/20211206134051/https://ipvm.com/reports/tiandy-iran-business?code=Fhsudb.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Kabanov Y (2020) The Interaction between ICT and Authoritarian Legitimation Strategies: An Empirical Inquiry. In Chugunov A, Khodachek I, Misnikov Y and Trutnev D (eds), *Electronic Governance and Open Society: Challenges in Eurasia*. Cham: Springer International Publishing, pp. 184–194.

Kerr JA (2018) Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region. *International Journal of Communication* **12**, 3814–3834.

Khabar Online (2023) Major General Salami: Last year's unrest was the strongest and most dangerous global fight against the Islamic regime of Iran. 1 August, https://www.khabaronline.ir/news/1796588.

Khalil L (2020) *Digital Authoritarianism, China and COVID*. Sydney: Lowy Institute.

Lamensch M (2021) Authoritarianism Has Been Reinvented for the Digital Age. Center of International Governance Innovation, 9 July, https://www.cigionline.org/articles/authoritarianism-has-been-reinvented-for-the-digital-age/.

Levitsky S and Way LA (2010) *Competitive Authoritarianism: Hybrid Regimes after the Cold War, Problems of International Politics*. Cambridge: Cambridge University Press.

Lilkov D (2020) Made in China: Tackling Digital Authoritarianism. *European View* **19**(1), 110–110. https://doi.org/10.1177/1781685820920121.

Liu KZ (2019) Commercial-State Empire: A Political Economy Perspective on Social Surveillance in Contemporary China. *The Political Economy of Communication* **7**(1), 3–29.

Maerz SF (2016) The Electronic Face of Authoritarianism: E-Government as a Tool for Gaining Legitimacy in Competitive and Non-Competitive Regimes. *Government Information Quarterly* **33**(4), 727–735. https://doi.org/10.1016/j.giq.2016.08.008.

Michaelsen M (2018) Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran. *International Journal of Communication* 19328036 **12**, 3856–3876.

Ming-Tak Chew M and Wang Y (2021) How Propagames Work as a Part of Digital Authoritarianism: An Analysis of a Popular Chinese Propagame. *Media, Culture and Society* **43**(8), 1431–1448. https://doi.org/10.1177/01634437211029846.

Morgenbesser L (2020) The Menu of Autocratic Innovation. *Democratization* **27**(6), 1053–1072. https://doi.org/10.1080/13510347.2020.1746275.

Morgus R (2019) The Spread of Russia's Digital Authoritarianism. In Wright ND (ed.), *Artificial Intelligence, China, Russia, and the Global Order Technological, Political, Global, and Creative Perspectives*. Maxwell AFB, AL: Air University Press, pp. 89–97.

Morozov E (2011) Whither Internet Control. *Journal of Democracy* **22**(2), 62–74. https://doi.org/10.1353/jod.2011.0022.

MTN Group Limited (2010) *Integrated Business Report for the Year Ended 31 December 2009. Book 2 – MTN Financial Statements*. Johannesburg: MTN Group.

Nokia (2023) Annual Report 2023. Helsinki, https://www.nokia.com/system/files/2024-03/nokia-annual-report-2023.pdf.

Nokia Corporation (2020) Annual Report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the fiscal year ended December 31, 2019, https://nokia.gcs-web.com/static-files/00042f0d-b423-401b-bc00-a523d72f8828.

Nokia Siemens Networks (2010) August 20, 2010 update: Response to lawsuit filed by Isa and Mehdi Saharkhiz against Nokia Siemens Networks (Archived). http://web.archive.org/web/20100824053938/http://blogs.nokiasiemensnetworks.com/news/2010/08/17/activist-sues-nokia-siemens-networks/.

NSO Group (2024) About Us. https://www.nsogroup.com/about-us/.

O'Donnell G (1978) Reflections on the Patterns of Change in the Bureaucratic-Authoritarian State. *Latin American Research Review* **13**(1), 3–38. https://doi.org/10.1017/S0023879100030661.

Pan J (2017) How Market Dynamics of Domestic and Foreign Social Media Firms Shape Strategies of Internet Censorship. *Problems of Post-Communism* **64**(3–4), 167–188. http://doi.org/10.1080/10758216.2016.1181525.

Papademetriou GT (2023) Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry. *Harvard Human Rights Journal* **36**, 191–221.

Pfeifer K (2016) Neoliberal Transformation and the Uprisings in Tunisia and Egypt. In Bahramitash R and Esfahani HS (eds), *Political and Socio-Economic Change in the Middle East and North Africa: Gender Perspectives and Survival Strategies*. New York: Palgrave Macmillan US, pp. 21–73.

Polyakova A and Meserole C (2019) *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Washington, DC: Brookings Institution.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Qin B, Strömberg D and Wu Y (2017) Why Does China Allow Freer Social Media? Protests Versus Surveillance and Propaganda. *Journal of Economic Perspectives* **31**(1), 117–140. https://doi.org/10.1257/jep.31.1.117.

Radio Zamaneh (2009) Outside Politics: Iran: Reconnecting SMS System after 40 Days. 23 August. *Radio Zamaneh*.

Ratner SR (2001) Corporations and Human Rights: A Theory of Legal Responsibility. *The Yale Law Journal* **111**(3), 443–545.

Reuters (2009) S. Africa's MTN denies report Iran network blocked. Reuters, 24 June, https://www.reuters.com/article/iran-election-mtn-idUSLO29259220090624.

Reuters (2017) Update 1: South Africa's MTN to invest $295 m in Iranian Net broadband network. 8 May, https://www.reuters.com/article/mtn-group-iran-idUSL8N1IA2VL.

Rodan G and Jayasuriya K (2009) Capitalist Development, Regime Transitions and New Forms of Authoritarianism in Asia. *The Pacific Review* **22**(1), 23–47. https://doi.org/10.1080/09512740802651003.

Saglam K (2022) The Digital Blender: Conceptualizing the Political Economic Nexus of Digital Technologies and Authoritarian Practices. *Globalizations* **21**(6), 1023–1040. https://doi.org/10.1080/14747731.2022.2131235.

Schatz E (2009) The Soft Authoritarian Tool Kit: Agenda-Setting Power in Kazakhstan and Kyrgyzstan. *Comparative Politics* **41**(2), 203–222. https://doi.org/10.5129/001041509X12911362972034.

Schlumberger O, Edel M, Maati A and Saglam K (2024) How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition: An International Journal of Comparative Politics* **59**(3), 761–783. https://doi.org/10.1017/gov.2023.20.

Seawright J (2016) The Case for Selecting Cases That Are Deviant or Extreme on the Independent Variable. *Sociological Methods & Research* **45**(3), 493–525. https://doi.org/10.1177/0049124116643556.

Shahrabi S (2017) The Fog of App Wars in Iran. *Journalism is Not a Crime*, 24 November, https://journalismisnotacrime.com/en/features/2119/.

Shukri S (2023) Digital Authoritarianism: Protecting Islam in Multireligious Malaysia. *Religions* **14**(1), 87. https://10.3390/rel14010087.

Sinkkonen E and Lassila J (2022) Digital Authoritarianism and Technological Cooperation in Sino–Russian Relations: Common Goals and Diverging Standpoints. In Kirchberger S, Sinjen S and Wörmer N (eds), *Russia–China Relations: Emerging Alliance or Eternal Rivals?* Cham: Springer International Publishing, pp. 165–184.

Stavrianakis A (2017) Playing with Words While Yemen Burns: Managing Criticism of UK Arms Sales to Saudi Arabia. *Global Policy* **8**(4), 563–568. https://doi.org/10.1111/1758-5899.12484.

Stavrianakis A (2023) Debunking the Myth of the 'Robust Control Regime': UK Arms Export Controls during War and Armed Conflict. *Global Policy* **14**, 121–130. https://doi.org/10.1111/1758-5899.13191.

Stirland S (2008) Cisco Leak: 'Great Firewall' of China Was a Chance to Sell More Routers. *Wired*, 20 May, https://www.wired.com/2008/05/leaked-cisco-do/.

Tansel CB (2018) Authoritarian Neoliberalism and Democratic Backsliding in Turkey: Beyond the Narratives of Progress. *South European Society and Politics* **23**(2), 197–217. https://doi.org/10.1080/13608746.2018.1479945.

Tansey O (2016) *International Politics of Authoritarian Rule, Oxford Studies in Democratization*. Oxford: Oxford University Press.

Taylor M (2022) *China's Digital Authoritarianism: A Governance Perspective*. Cham: Springer International Publishing.

Tehran Bureau (2022) The Chinese companies building Iran's surveillance state. Tehran Bureau, 30 September, https://tehranbureau.com/the-chinese-companies-building-irans-surveillance-state/.

TeleGeography (2023) MTN Irancell has pumped more than USD10bn into Iran since launch. *TeleGeography Comms Update*, 2 February, https://www.commsupdate.com/articles/2023/02/02/mtn-irancell-has-pumped-more-than-usd10bn-into-iran-since-launch/.

Tiandy Iran (2021) Successful Projects (Archived). https://web.archive.org/web/20211126090445/https://tiandy.ir/successful-cases-iran/.

Tolstrup J (2015) Black Knights and Elections in Authoritarian Regimes: Why and How Russia Supports Authoritarian Incumbents in Post-Soviet States. *European Journal of Political Research* **54**(4), 673–690. https://doi.org/10.1111/1475-6765.12079.

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press

Tomashevskiy A (2017) Investing in Violence: Foreign Direct Investment and Coups in Authoritarian Regimes. *The Journal of Politics* **79**(2), 409–424. https://doi.org/10.1086/688356.

Treisman D and Guriev S (2015) How Modern Dictators Survive: Co-Optation, Censorship, Propaganda, and Repression. *SSRN Electronic Journal*, 1–36. https://extranet.sioe.org/uploads/isnie2015/guriev_treisman.pdf.

Uddin R (2022) Saudi Arabia's Neom megacity dreams get wilder, enriching foreign consultants. *Middle East Eye*, 15 July, https://www.middleeasteye.net/news/saudi-arabia-neom-megacity-enrich-foreign-consultants.

U.S. Department of Commerce (2022) Additions and Revisions to the Entity List and Conforming Removal from the Unverified List – Docket No. 221209-0267. https://www.federalregister.gov/documents/2022/12/19/2022-27151/additions-and-revisions-to-the-entity-list-and-conforming-removal-from-the-unverified-list.

U.S. Department of the Treasury (2023) Treasury Targets Vast Supreme Leader Patronage Network and Iran's Minister of Intelligence. 18 November, https://home.treasury.gov/news/press-releases/sm1185.

von Billerbeck S and Tansey O (2019) Enabling Autocracy? Peacebuilding and Post-Conflict Authoritarianism in the Democratic Republic of Congo. *European Journal of International Relations* **25**(3), 698–722. https://doi.org/10.1177/1354066118819724.

Wang M (2021) China's Techno-Authoritarianism Has Gone Global. *Foreign Affairs*, 8 April, https://www.foreignaffairs.com/articles/china/2021-04-08/chinas-techno-authoritarianism-has-gone-global.

Wintrobe R (1998) *The Political Economy of Dictatorship*. Cambridge: Cambridge University Press.

Zhihui C (2016) Nowhere to hide: Building safe cities with technology enablers and AI. Huawei, July, https://www.huawei.com/en/huaweitech/publication/winwin/ai/nowhere-to-hide.

Cite this article: Conduit D (2025). Digital Authoritarianism and the Global Technology Industry: Evidence from Iran. *Government and Opposition: An International Journal of Comparative Politics* **60**, 751–772. https://doi.org/10.1017/gov.2024.31

https://doi.org/10.1017/gov.2024.31 Published online by Cambridge University Press