Transnational State-Corporate Symbiosis of Public Security: China's Exports of Surveillance Technologies

Transnational State-Corporate Symbiosis of Public Security: China's Exports of Surveillance Technologies

Ausma Bernot
Griffith University, Australia

Abstract

Over the last two decades, the emerging Chinese Party-state has used commercial ties with North American and European providers of surveillance technologies to grow national prowess of public security, fostering a transnational state-corporate symbiosis. The exports of surveillance technologies from the Global North to China started in the late 1970s, and now Chinese technology companies are competing with and replacing those suppliers in the globalized neoliberal market. This research explores the two-way dynamic of China's state and private surveillance capacity underscored by international companies' profit-seeking behaviors and domestic technological and economic growth. Four case studies of companies from Canada, China, and the US are used to highlight the changing dynamics in the global circulation of surveillance technologies. Particular attention is paid to the cyclical nature of such technologies through which unresolved issues of global governance continue to emerge and, accordingly, support the growth of technology-powered authoritarianism worldwide.

Keywords

Authoritarian neoliberalism; China; globalization; high policing; state-corporate symbiosis; surveillance technologies.

Please cite this article as:
Bernot A (2021) Transnational state-corporate symbiosis of public security: China's exports of surveillance technologies. *International Journal for Crime, Justice and Social Democracy.* Advance online publication. https://doi.org/10.5204/ijcjsd.1908

Introduction

One thing tech companies cannot do, in my opinion, is involve themselves in politics of a country.
John Chambers, former chairman and CEO of Cisco (Forbes 2007)

This paper presents empirical findings from four companies in Canada, China, and the US to demonstrate how surveillance technology sales to police and public security agencies have been bolstered by the global regulatory trade environment and globalized markets since the dawn of telecommunications and computer technologies in the 1970s. The theory of the state-corporate symbiosis highlights how building China's state and private surveillance capacity is a two-way dynamic underscored by Global North companies and their profit-seeking behaviors and domestic technological and economic growth.

First, the paper outlines the theoretical foundations of the state-corporate symbiosis within transnational security markets and highlights their use in state securitization and the social justice harms those connections may create. It then positions China's growth within the surveillance technology market, describes the study's methodology, and presents the analytical results. The discussion shows that surveillance technologies are not politically neutral but rather part of "high policing" strategies of surveillance bolstered by global trade and national alliances. This is shown in the context of growing Chinese technological prowess and influencing global relations.

Surveillance Technologies and State-Corporate Symbiosis

The unrestricted growth of surveillance systems has brought capitalism and democracy into conflict by expanding unrestricted and unmonitored surveillance networks (Lyon 2015). In democratic countries, the implications of expanding surveillance networks have encumbered democratic rights, such as privacy and freedom of speech (Brodeur and Leman-Langlois 2006; Lyon 2015); authoritarian countries can use surveillance to insulate the power of the political leaders from unrest (Griffiths 2019; Xu 2021). As such, surveillance technologies used by security agencies, public or private, have assumed an increasingly politicized role, pushing national governance towards neoliberal authoritarianism. For example, the US and Canada have embraced constitutional and legal changes to insulate the state from social and political instability during global financial crises (Bruff 2014). Simultaneously, several Asian economies, such as China and Singapore, achieved rapid economic growth by pairing their authoritarian systems of governance with the neoliberal aspects of market regulation (Juego 2018).

Such changes in the global political economy allowed for the state-corporate symbiosis to emerge within transnational networks of the security industry (O'Reilly 2010). O'Reilly's theory of the state-corporate symbiosis addresses the blurring of public and private policing terrain, where private actors of transnational security play a key role in building state-corporate security mechanisms. O'Reilly and Ellison (2006) have coined the term *private high policing* to conceptualize the emergent trend of policing based on risk, increasingly *un*-linked from state actors and connected to providers of corporate security services. The authors propose that this new type of high policing develops when "public and private high policing actors cross-permeate and coalesce in the pursuit of symbiotic state and corporate objectives" (O'Reilly and Ellison 2010: 641). They expand the term high policing (Brodeur and Leman-Langlois 2006), referring to political surveillance with the aim to preserve the political regime, which maintains relevance in modern China. A running thread in surveillance systems of high policing is the "ethos of total control" that allows authorities to control information (Marx 2018). Following this line of theoretical thought, this paper locates China's economic and political growth in the context of shifts in the global supply of security technologies, focusing on the multipolarity of global leadership (Fouskas and Gökay 2019).

Foster and McChesney (2014) have observed that the phenomenon of rapid development of surveillance technologies was supported by neoliberal policies and the globalization of markets. In particular, the US has benefited from selling warfare and security products since the 1940s. The neoliberal reforms of the

1980s further diminished the economic role of the nation-state, increasing that of private companies. In the 1970s, the changing leadership of China opened the country to international trade, and mature economies obtained the opportunity to sell their surveillance products without accounting for political implications.

Fitting itself with neoliberalism at a discursive level, China established itself as a trade partner that does not meddle in national political affairs while simultaneously trading surveillance technologies that heighten the surveillance capacity of political regimes and afford high policing. The Chinese Party-state[1] has encouraged economic growth and political non-interference in building national alliances through trade (Nathan 2015). Bernat and Whyte (2017) have named these regulatory pathologies a *regime of permission*—a normalized regulatory regime that prioritizes the uninterrupted accumulation of capital, allowing state-corporate crime to occur. Political scientist Minxin Pei (2018) found that US$77.8 billion (36% of total investments) of Chinese foreign infrastructure investments has linked China with authoritarian countries. China's increasing embeddedness in the global economy has thus raised national security concerns overseas because of the country's explicit support for authoritarian leaders (Cave et al. 2019).

International pressure against the free trade of Chinese surveillance technologies has backfired in two ways. First, Chinese President Xi Jinping has criticized other countries for politicizing and weaponizing supply chains and encouraged the central government to reduce national dependence on imports (Center for Security and Emerging Technology [CSET] 2020). Second, Chinese companies selling surveillance technologies, now limited in international trade and financing options, are likely to seek increased support from the government and explore new markets. In the early 2000s, western companies faced political pressures for selling surveillance technologies to China. Still, they could ultimately defy those political pressures by leveraging their legitimate business rights within the globalized neoliberal markets. Similarly, Chinese companies are now defending their business interests to sell surveillance products globally without "politicized" constraints (Huawei 2020; CSET 2020). The geopolitical rivalry of surveillance technology trade is not only shifting trade relationships but will also likely polarize the transnational political landscape.

Locating China's Growth of Surveillance Technologies in the Global Context

China has been a recipient of internationally traded surveillance technology supplies since the 1970s, even before the economic reforms began and the Party-state set modernization aims for systems of public security and policing. With the adoption of the internet and digital technologies, surveillance was first identified as an important means to uphold social and regime stability (Griffiths 2019). The accession to the World Trade Organization in 2001 was pivotal in the growth of China's trade power (Bhattasali, Li and Martin 2004). Membership and, eventually, leadership in international governance organizations positioned China as a global decision-maker among other large economies in the world (Jayasuriya 2006). The formation of China's political power cannot be separated from the rejuvenation of national identity. In 2013, Xi Jinping's ascent to the Communist Party of China (CPC) presidency signposted a new era of China's power. He revitalized the CPC through a multitude of state-strengthening capabilities and expanded the scope of surveillance technologies, such as consolidating a closed-loop relationship between surveillance technology providers and state access to information (Creemers 2017; So 2019: 53).

In 2017, Chinese authorities proposed a strategic blueprint to support Chinese artificial intelligence (AI) companies to become global industry leaders by 2030 (Larson 2018). Furthermore, surplus capital reinvested through the Belt and Road Initiative (BRI) has created sales opportunities for Chinese manufacturers by providing support for infrastructure projects of its partner countries, with a focus on Central Asia and Eastern Europe (Yu 2017). The BRI includes the exports of digital technologies to Zimbabwe, Venezuela, and Belarus (Cave et al. 2019). Such exports bolster high surveillance of authoritarian-leaning countries under the "principle of indifference," through which state actors can be insulated from seeing the harm their products create (Lasslett, Green, and Stańczak 2015). By coupling

political and trade relations, China built international alliances and entered global mechanisms of governance. If implemented successfully, the BRI has the capacity to reshape the geopolitical and economic landscape in Asia and globally (So 2019).

Methodology

This paper analyzes four case studies of surveillance technology companies from Canada (Nortel), the US (Cisco), and China (Huawei and Megvii) to understand how national and international developments have enabled the global circulation of surveillance technologies and shaped China's position in the global market. These companies were selected because they have been involved in political debates about the sales of their surveillance technologies (Dai 2019a; Griffiths 2019; Walton 2001).

The embedded multi-case study method was used in this research study, with documents as the unit of analysis. This method is commonly used to understand the dynamics and processes in organizations (Mills, Durepos, and Wiebe 2012; Lasslett, Green, and Stańczak 2015). Similar to a time series approach, the cases qualitatively followed a theoretically significant trend of state-corporate security nexus over time, with Nortel as the oldest entrant to the Chinese security market and Megvii as the newcomer. The need to include possible alternative explanations is important. Therefore, four different organizations were selected for this analysis (Yin 2018). The types and number of data sources are outlined in separate tables for each case study.

Table 1. Case study definitions and details

	Nortel	***Cisco***	***Huawei***	***Megvii***
Case description	Nortel, a Canadian company with a Chinese merger, is a long-time supplier of **network technology** to China.	Cisco is a US-based company that has long been a supplier of **network and communications technologies** in China, with police agencies being its stable customer base.	Huawei is a Chinese technology giant with headquarters in China and multiple subsidiaries overseas. Huawei was the first to fully develop **5G technology** globally at competitive prices.	Founded in 2011, Megvii is a China-based company that develops and produces deep-learning and image recognition technologies, such as **Face++**.
Number of documents analyzed	63	62	75	78
Assigned themes	Business in China; Investment in China; Contributing to censorship; Hacking concerns; Business neutrality	Business in China; Relationships with the Party-state; Investment in China; Business neutrality; IP battle; Espionage; International laws and regulations	Business development; Technological excellence; Relationships with the Party-state; Market advantage; Security concerns; Business neutrality; Pressure from the US; Trade with authoritarian countries	Business development; Innovation; Government support; Pressure from the US; Allegations of human rights violations; Ethics

This study consulted over 300 open-source online data sources, company documents, and academic publications, which were analyzed qualitatively by coding and deriving themes. The search was run from 2000 to 2020. Repeated or republished sources were only included once. For Nortel and Cisco, the English language search was conducted by searching for the company name with the word "China" added to the search string. For a Chinese language search, the companies' Chinese names were searched (e.g., 思科 for

Cisco and 北电 for Nortel). For Chinese companies, the English search and Chinese language search included a specific technology that the companies sell internationally (e.g., 5G for Huawei and Face++ for Megvii).

This study has inductive and deductive elements for incorporating data- and theory-driven codes (Linneberg and Korsgaard 2019). Several types of data were used for data type triangulation to support the internal validity (Mills, Durepos, and Wiebe 2012), which is important in the context of international trade with China since state-level information may differ from corporate opinions. First, official data about a selected product of each company, such as annual reports, was sourced to determine the scope and size of company operations. Second, a news search in English and Mandarin was conducted to determine the exact technologies of the exports. Last, a search of academic articles and government documents was conducted. The documents were first selected deductively, focusing on the state-corporate symbiosis and high policing aspects of surveillance technology exports in the global trade context:

- Technologies exported to China (case studies 1 and 2) and from China to other countries (case studies 3 and 4);
- Company connections to the Party-state of China;
- International trade policies, initiatives, and organizations that have supported the global trade of surveillance technologies.

A multi-case study method advises employing a qualitative analysis that best suits the needs of the research project (Yin 2018). Here, a thematic analysis was applied to study common themes and patterns in triangulated research data. Each theme consolidated had appeared in texts multiple times, and the coding stopped when it yielded no new information for the research aim and when thematic saturation was achieved (Saunders et al. 2018). The research study followed the six-step data analysis process of initial familiarization of the data by reading and re-reading the data, generating initial codes, searching for initial themes, reviewing the emergent themes, naming and defining the themes, and the final analysis (Braun and Clarke 2006).

Case Study Descriptions

Nortel Company Background

The Nortel Networks Corporation was a Canadian telecommunications and data networking equipment manufacturer. The company was a supplier of telecommunications technologies in China from the 1970s, helping the country build its communications infrastructure. Nortel chose to enter the Chinese market with a localized strategy and was one of the first companies to do so. Nortel Networks China was founded in 1972. In 2001, the company reported US$1.6 billion in revenue in China and employed 2,600 people (Fan 2006). In the early 2000s, the company's business plummeted. Nortel filed for bankruptcy in 2009 and settled in 2017 (Kehoe 2014; The Canadian Encyclopedia 2018). Nortel's business in China has two main characteristics: the localization strategy to generate sales and leveraging national interests to consolidate business relationships.

Cisco Company Background

Similar to Nortel, Cisco Systems has contributed to the construction of surveillance in China. Cisco entered the Chinese market in 1994 and had secured 30% of the country's market for internet routers by 2008, employing 3,000 people (Cisco 2008). The company has been one of the largest suppliers of networking equipment that has supported building the Great Firewall of China that censors the internet domestically (Walton 2001). It continues to do business there with significant competition from Huawei. In 2003, Cisco filed a lawsuit against Huawei for allegedly infringing and misappropriating Cisco's trade secrets and intellectual property, dropping the lawsuit in 2004 when Huawei pledged to modify its offerings of contested products (Hamblen 2004; U.S.–China Economic and Security Review Commission 2011: 15). Interestingly, Cisco's relationship with China worsened because the company was found complicit in American espionage in China. In 2014, China retaliated further by removing Cisco's 60 products from the Chinese preferential national procurement list (Carsten 2015).

Huawei Company Background

Huawei Technologies Co., Ltd. is a giant Chinese developer and manufacturer of information communications technologies (ICT) and one of the few Chinese ICT companies that have entered the global marketplace. Founded in 1987, it first confined itself to the domestic market. However, the company secured US$10 billion and US$30 billion credit lines with the China Development Bank to support sales outside China in 2004 and 2009 (McMorrow 2019). In 2010, Huawei was listed in *Fortune 500* with annual revenue of US$21.8 billion (Fortune 2020). The emergence of 5G technology created a "blue ocean" opportunity for the international trade of ICTs, and China rapidly climbed to a position of leadership. The US–China trade war started in 2018, and Huawei's 5G technology became the centerpiece, resulting in bans in multiple countries (Kaska, Beckvard, and Minarik 2019). Currently, the debates are focused on national security concerns in the US, whereas, in China, they cite the protectionism and loss of trust in the US as a global communications technology supplier.

Megvii Company Background

Megvii (旷视) is a developer and manufacturer of image recognition and deep-learning software and the leading provider of the facial recognition product Face++ in China. The company has applied its technology to personal Internet of Things (IoT), city IoT, and supply chain IoT, with the Chinese market as the first market entry priority and plans to expand internationally (Dai 2019a). Founded in Beijing in 2011, it is the youngest of the four case study organizations. Megvii is financed by China mega-corporations Alibaba and Ant Financial, as well as the Bank of China, among other investors. It is valued at approximately US$4 billion (Shu 2019). Among China's *four little dragons of AI* or unicorn startups,[2] Megvii was the first to launch their initial public offering (IPO) request on the Hong Kong Stock Exchange (Chen 2020a). In 2018, Megvii held 20.6% of China's US$1.76 billion AI market (Internet Data Center 2020), and Face++ technology was used in over 220 countries and regions. Internationally, the company's image recognition testing has won against Microsoft, Facebook, and Google's products at the 2018 International Conference on Computer Vision.

Results

The results showcase the key thematic findings connected to the theoretical framework of the state-corporate symbiosis. Strategic political connections and support for Chinese high policing were found as important and financially rewarding for companies when targeting sales in China. Furthermore, the discursive neutrality of business and technology rewarded Cisco and Nortel, while Chinese companies were labeled as threats to national security despite efforts to increase business transparency. The implications of these patterns are explored in the discussion section.

Strategic Political Connections

Strategic political connections were important for all companies in the case studies when working with the Chinese government. If the companies could align their developmental goals to the Chinese national strategic priorities, they were supported by the government, signaling the state-corporate symbiosis.

In 1998, Nortel secured seven contracts for intelligent networks, ATM networks, and broadband in China, totaling US$120 million (Department of Foreign Affairs and International Trade [DFAIT] 1998). The company's business developed through securing projects such as the US$10 million Shanghai citywide fiberoptic broadband network, which enabled the authorities to monitor network users through a censored firewall (Walton 2001). An independent security report by Walton (2001) listed multiple public security projects to which Nortel contributed, most prominently a database-driven remote surveillance system that censors communications and tracks people in China. Up until the dissolution of Nortel's business operations, China Nortel Manager Jerry Huang was responding to market needs for improving security and data management by positioning Nortel as a supplier with the capacity to meet those needs (M2 Presswire 2009).

Leveraging bilateral political interests also helped the company bolster national-level bilateral relationships. In 1998, Nortel signed an agreement with the leading Tsinghua University in Beijing to establish a joint research lab for developing networking technologies (ResponseSource 1998, Tsinghua University 2018). By 2008, the research laboratory was well established and developing speech recognition technologies (Vitaliev 2008). Nortel could facilitate national-level political meetings between Canada and China by enrolling in strategic collaborations within the Chinese security space, thus strengthening bilateral relationships (DFAIT 1998).

The China-based surveillance technology companies also strongly benefited from aligning themselves with the political goals of the Party-state. In 2019, the Party-state determined that building information infrastructure would be the BRI's priority, opening opportunities for Huawei to align their international growth strategy with the national strategy (Zhang 2019). A recent congressional briefing presented by the U.S. Committee on Foreign Relations posited that China has been "developing an authoritarian governance model for the digital domain" (SFRC Democratic Staff 2020), and Huawei is a company behind that shift. In 2018, the company received US$222 million in Chinese government grants, linking the company to the interests of the Party-state (SFRC Democratic Staff 2020: 25). Being aligned with China's national goals has strengthened Huawei's price and value proposition for its 5G product as China's political power expanded internationally under the leadership of Xi Jinping (Yu 2017). Huawei's surveillance technologies modernized the state capabilities of high policing embedded within the state-corporate security nexus, allowing for the Chinese Party-state to strengthen social control without direct coercion (Xu 2021).

Megvii's company vision similarly aligns well with national ambitions of technological modernization, allowing Megvii to access national funding (Sun 2018). Reportedly, 64% of Megvii's revenue comes from selling its technologies to Chinese government entities (Chen 2021). Because the Chinese government aims to become a global AI leader, the launch of the tech innovation board on the Shanghai Stock Exchange is one possible alternative for domestic companies to obtain investments (Lim 2020). Megvii applied to publicly list its company in 2021 (Chen 2021).

Regime of Permission and its Boundaries

The practices of trade non-interference do not extend to Chinese companies selling internationally but permit technology companies from the Global North to contribute to China's surveillance capacity growth. Bernat and Whyte (2017) have named state-corporate collaborations that seek uninterrupted capital flows a "regime of permission" and argued that regimes of permission might allow for wider social harms to emerge. It is reasonable to monitor China's sales of surveillance technologies that openly support authoritarian countries. However, the same regulatory zeal should apply to companies from the Global North. This duality of the international regime of permission pushed Huawei and Megvii to seek commercial alliances with countries that hold political ties with China or are authoritarian-leaning.

Interestingly, for the organizations included in these case studies, the regime of permission only extended one way: The North American companies of Nortel and Cisco were able to freely trade their technologies in China and deflect security concerns. Nortel benefited from its early entry into the Chinese market and continued to supply network technology to politically sensitive projects in China until the company's closure in 2017. Internationally, there was no debate on the consequences of supplying key networking infrastructure to China from overseas due to two reasons. First, in the 1970s, many believed that China was opening its political space by reforming the economy. Second, within the regime of permission, Nortel's business was considered legitimate. The company operated in China for more than two decades (Walton 2001).

Many believed that the internet would bring greater freedom to China (MacKinnon 2011). Bill Clinton commented that restricting communications on the internet would be as impossible as nailing Jell-O to a wall (Griffiths 2019). The early 2000s proved him wrong—it could be done with the help of North American companies. In 2000, the Chinese Ministry of Public Security organized the *2000 Security China Expo*, during which it aligned national development with advancing the development of surveillance

technologies. Among others, Cisco, then a major supplier of network technology in the US and growing presence in China, attended the expo and consolidated supply relationships with national security agencies entering preferential tender lists (Walton 2001). A leaked 2002 presentation from the Cisco sales team in China suggests that their sales pitch was based on the priorities of the local police departments and offered help in implementing their strategic goals, including censorship (Lai Stirland 2008). In response, Cisco claimed that it was a mistake of a local sales agent and did not represent the company's views (Lai Stirland 2008). Nonetheless, the leaked presentation attracted attention to the fact that Cisco was a building block of Chinese public security.

On the opposite end, Huawei's bid to acquire Nortel's fiberoptic equipment in 2009 was met with security concerns for operators in North America carrying Nortel's equipment (Greenberg 2009), signaling that the regime of permission only extends to the Global North. In 2011, the U.S.–China Economic and Security Review Commission noted that such a purchase might be blocked over security concerns of the "distressed company's customers" (U.S.–China Economic and Security Review Commission 2011: 55). Megvii similarly found the boundaries of the state-corporate regimes of indifference as the company was penalized by the regulatory regimes in the Global North that allow unregulated exports of surveillance technologies to China but control the imports of such technologies from China. In 2018, Megvii applied for a $500 million IPO in the Hong Kong Stock Exchange, allowing transparency to its business operations and revenue. Shortly after, the Human Rights Watch published a report identifying Face++ as the technology used in a policing app in Xinjiang and called for a US export ban on technology companies collaborating with the Chinese government, including Megvii (Human Rights Watch 2019). After Megvii denied the allegations, the report was checked and amended. Nonetheless, in October 2019, Megvii was one of eight Chinese companies and 20 government entities barred from buying US technology without approval from the U.S. Department of Commerce due to their alleged involvement with human rights abuses of ethnic minorities in the Xinjiang region (Shen 2019). When asked about involvement in Xinjiang, CEO Yin Qi commented that Megvii focuses on the "commercial, not political" but confirmed that 1% of its revenue was from Xinjiang in 2018 (Dai 2019a; Franklin and Zhu 2019).

After the publication of the US Entity List, major international co-investors in Megvii, such as Goldman Sachs, reconsidered their involvement with the company (Franklin and Zhu 2019; Shen 2019). This has impacted Megvii's business revenue. In the first half of 2019, Megvii had tripled total sales and made CNY$694.8 million (US$97 million). However, Bloomberg reported only a 2.7% estimated growth in the second half of 2019 (Chen 2020b). The Hong Kong IPO funding round lapsed after the company failed to achieve the expected revenue amidst inclusion in the US Entity List as a security threat and the global COVID-19 pandemic (Lim 2020). This put the company at a crossroads of choosing between international expansion or prioritizing national development. In 2020, Megvii established an independent open-source framework to build AI solutions to reduce reliance on products from the US, signaling its choice (Udemans 2020).

Discursive Neutrality of Business and Technology

All companies in the case studies defended the technological and business neutrality of the surveillance technologies they were selling. This further showcases how surveillance technology companies use discursive and regulatory tools to tap into regimes of indifference and deflect the possibility of social harm they may create. While Nortel and Cisco were protected by the neoliberal policies of their home markets, the Chinese companies of Huawei and Megvii put additional efforts to prove the security and trustworthiness of their technologies when selling internationally. The two companies were eventually pushed to focus more on politically aligned markets.

Cisco's company illustrates how they harnessed the discourse of business neutrality while actively contributing to increased censorship in the country. John Chambers firmly established Cisco as a key actor in building network infrastructure in China by attending Chinese trade expositions and fairs, aligning the company with national development goals, and maintaining discursive neutrality. The US Council on Foreign Relations found that the technological censorship infrastructure in China became more effective

in 2004 because technology companies from the US supported it; Cisco secured US$100 million from that contract to provide backbone network equipment for 200 cities nationwide (Business Wire 2004, Cisco 2004). In the 2006 backlash, the U.S. House Subcommittee on Human Rights and International Relations directly challenged Cisco by investigating human rights abuses supported by their technology (Griffiths 2019). Then, the president of Cisco, John Chambers, chose to defend the company's right to business neutrality: "One thing tech companies cannot do, in my opinion, is involve themselves in politics of a country" (Forbes 2007). In another congressional hearing held in 2008, Cisco again defended their right to supply networking technologies to China (Hickey 2008). In 2011, Cisco signed a deal to build the infrastructure for CCTV surveillance in Chongqing city (Cohn and York 2011).

Huawei, now a significant competitor of Cisco in the Chinese market, faced a different market environment. Huawei's swift development and growing market share in the global technology supply, especially in the case of 5G, triggered allegations that the company is a threat to national security globally. In 2018, a meeting of the Five Eyes intelligence network of the United States, Canada, Australia, New Zealand, and the UK led to internationalization restraints of Huawei's 5G technology (Uhlmann and Grigg 2018). In the same year, the US president signed a National Defense Authorization Act banning the sales and use of Huawei products in the US based on concerns of connectivity sabotage or denial of service attacks (Jaisal 2020). In 2019, the NATO Cyber Defence Centre report identified Huawei's 5G technology as a security risk, highlighting Huawei's ties with the Chinese government (Kaska, Beckvard, and Minarik 2019). Huawei filed a lawsuit against the US government to "protect its legitimate rights and interests through the proper channels" (Huawei 2020: 8). Ken Hu Houkun, the rotating chairman of Huawei, spoke against the politicization of 5G business and to technological neutrality to defend its right to global supply, stating "politicizing the issue is a bigger challenge, not only for Huawei but also for the wider industry and for trade relations on a large scale" (Chen 2019).

Internationally, similar to Cisco and Nortel, Huawei spokespeople have used the idea of technological neutrality. Restrained by the markets in the Global North, the company harnessed Global South alliances to increase sales. Despite the ongoing legal and political debates, Huawei has leveraged its global connections and maintained traction in the Association of Southeast Asian Nations (ASEAN) countries, Latin America, Africa, and the Gulf region. According to Huawei's 2019 annual report, the company made CNY$206,007 million in annual revenue from Europe, the Middle East, and Africa and exported the 5G technologies to over 300 projects in 20 industries and 50 operators and supplied over 40,000 5G base stations (Huawei 2020). Huawei has been welcomed to supply its 5G technology to the Gulf and ASEAN countries, which proposed to exclusively adopt Huawei's product if it was offered at a competitive price (Al Fayad 2019). The 5G technologies were also exported to countries that the US holds sanctions against, including Iran, Syria, North Korea, and Cuba (Galbraith 2019; Inkster 2019). In the context of the decline of North American political influence over trade relations, Chinese companies thrive under China's discursive principle of non-interference. On a national level, the Chinese Party-state reacted to international trade restrictions posed on China by encouraging accelerated domestic spending and the substitution of imported components (CSET 2020).

Among the case studies, Megvii is the only company that addressed the possible negative impacts that their technology might have if adopted for the purpose of suppression (Megvii 2020). Yin Qi has acknowledged that their technology processes sensitive data without an industry-wide standard on user privacy but believes that the benefits of the technology outweigh the drawbacks (Sun 2018). In 2019, the company launched an ethics committee to prevent the weaponization of its technology (Dai 2019b). However, the company dropped the Hong Kong IPO applied to be publicly listed on the Shanghai Stock Exchange, signaling an increased focus on the Chinese domestic market.

Discussion

The empirical evidence of the state-corporate security symbiosis in China raises issues concerning the regulatory regimes of international trade in surveillance technologies. The four case studies, analyzed in a

sequential timeline, draw from the theory of the state-corporate symbiosis to showcase how the economic and technological development of surveillance capacity in China has been supported by the unregulated international trade of surveillance technologies. This is the first research paper to analyze how international trade dynamics constrain Chinese technology companies and the repercussions that stem from that.

Surveillance technology companies from the Global North have been selling their products and services in China from as early as the 1970s, protected by the regulatory regimes of indifference and discursive technological and business neutrality (Bernat and Whyte 2017; Carsten 2015; Forbes 2007). Marx (2014) has articulated the inherently political nature of surveillance technologies via the concept of high policing. In democratic countries, high policing strategies are meant to upkeep democratic values with varying degrees of success. Meanwhile, in authoritarian countries, high policing supports the power-ruling actors, insulated from the broader society. O'Reilly and Ellison (2006) have argued that this is less applicable in western democracies, where policing is increasingly outsourced to private actors, whereas in China, the political stability of the Party-state benefits from adopting digital surveillance (Xu 2021). If surveillance technology companies align themselves with the country's national goals, they are supported by the Party-state. Such companies are provided state subsidies, advantageous access to the Chinese market, and preferential tender lists (Yu 2017; Zhang 2019).

On a broader geopolitical scale, the global governance framework restricts the trade opportunities of Chinese companies while rewarding surveillance technology providers from the Global North within state-corporate regimes of indifference. In recent years, protectionist policies, trade bans, and allegations of human rights abuses have diminished Chinese companies' business prospects with western countries (Ashooh 2019; Fajgelbaum et al. 2020). As the case studies of Huawei and Megvii show, this has resulted in two outcomes. First, the Chinese Party-state is building self-dependency (CSET 2020, Udemans 2020). For example, recent protectionist measures applied by the US have observed retaliation from trade partners, and China has drafted a national-level strategy to reduce dependence on US supply chains (CSET 2020; Fajgelbaum et al. 2020). Second, at a national level, the Chinese Party-state and private companies draw on trade deals to build alliances with other countries, such as the Gulf region (Al Fayad 2019; Chen 2019; Huawei 2020). Some of these countries have authoritarian leaders that welcome Chinese investments without reservations about human rights (Pei 2018). O'Reilly (2010: 201) has argued that the "state-corporate symbiosis reflects the loci of power in the neoliberal context," which is observed in the emergent trend of authoritarian neoliberalism. China has built international ties and created opportunities for national giants and technology unicorns to export their surveillance technologies by discursively promoting state sovereignty and non-interference in its trade practices, even if used for censorship and political repression (Nathan 2015).

From a broad perspective, the global order is shifting towards multipolarity, emergent economies, and China's rising position in global governance and trade (Fouskas and Gökay 2019; Jayasuriya 2006). The remodeling of global wealth and economic and political alliances suggests a turn towards authoritarianism. Furthermore, the rules of global governance are decided by a network of large economies that now include China (Berberoglu 2020; Jayasuriya 2006; Murakami Wood 2017; So 2019).

Conclusion

The theory of the state-corporate symbiosis directs its attention to how surveillance technologies are bought from and sold to China. It articulates how the regime of indifference—a characteristic of state-corporate nexuses (Bernat and Whyte 2017)—does not extend to Chinese technology companies, thus encouraging authoritarian-leaning alliances. However, surveillance technology companies from the Global North can profit from harnessing the regime of indifference to align themselves with the national goals of the Chinese Party-state. The growth of technological capacity and resulting social harm are not a "China problem" but rather a problem of the globalized regulatory system that supports the transnational trade of surveillance technologies. Guided by capitalist values over social values, state-corporate nexuses rely

on increasingly symbiotic relationships (Tombs 2012). This is especially pertinent to high-tech surveillance technologies that require an advanced level of technical expertise and cannot be solely implemented and operated by state actors. Such technologies operationalize strategies of high policing and are inherently political.

The macro perspective of the case studies showcases how China has leveraged political and economic initiatives to fuel and sustain national economic growth and bolster the technological capacities of high policing. This process also highlights how the rules of the global capitalist order have supported and legitimized that growth. Since the 1980s, the globalized neoliberal market has allowed technology companies from the Global North to benefit from transnational trade. In that time, authoritarian countries that adopted neoliberal aspects of market economies have grown economically (Juego 2018). Restricted in the Global North, Chinese technology companies are creating ties with other authoritarian countries under the guise of the discursive principle of non-interference while simultaneously bolstering high policing strategies with advanced surveillance technologies.

The fact that this is of concern to the leaders in the Global North reveals a deep-seated problem of globalized trade markets. The denialist opinion of former chairman and CEO of Cisco, John Chambers, that technology companies cannot involve themselves in the politics of a country is simply not borne out by empirical evidence. Surveillance technologies used by security agencies are not politically neutral. Rather, they are inherently political, and their trade calls for transparency, accountability, and regulation both in China and internationally.

Acknowledgments
I want to thank Muhammad Amrat Saeed and Shivam Arora for the early conceptual conversations and extend my gratitude to Phyu Phyu Oo, Regina Ganter, Andrew Childs, and the two anonymous reviewers for their comments on the drafts of this paper.

Correspondence: Ausma Bernot, PhD Candidate, School of Criminology and Criminal Justice, Griffith University, Building M10, 176 Messines Ridge Road, Mt Gravatt QLD 4122, Australia. ausma.b@gmail.com

[1] In this study, I use *Party-state* to refer to the CPC and Chinese government.
[2] Unicorn startups are privately owned startups at a valuation of over US$1 million.

References

Al Fayad FS (2019) Huawei and the Gulf region: Market opportunities despite the ongoing US-China trade war. *International Review of Management and Marketing* 9(4): 47–53. https://doi.org/10.32479/irmm.8206

Ashooh RE (2019) Addition of certain entities to the entity list. *Federal Register*. https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

Berberoglu B (2020) *The global rise of authoritarianism in the 21st century: Crisis of neoliberal globalization and the nationalist response*. New York, NY: Routledge.

Bernat I and Whyte D (2017) State-corporate crime and the process of capital accumulation: Mapping a global regime of permission from Galicia to Morecambe Bay. *Critical Criminology* 25: 71–86. https://doi.org/10.1007/s10612-016-9340-9

Bhattasali D, Li S, and Martin W (2004) *China and the WTO: Accession, policy reform, and poverty reduction strategies*. Washington, DC: World Bank and Oxford University Press. https://openknowledge.worldbank.org/handle/10986/14920

Braun V and Clarke V (2006) Using thematic analysis in psychology. *Qualitative Research in Psychology* 3(2): 77–101. https://doi.org/10.1191/1478088706qp063oa.
Brodeur JP and Leman-Langlois S (2006) Surveillance fiction or higher policing? In Haggery KD and Ericson R (eds) *The new politics of surveillance and visibility*: 171–198. Toronto, ON: University of Toronto Press.
Bruff I (2014) The rise of authoritarian neoliberalism. *Rethinking Marxism* 26(1): 113–129. https://doi.org/10.1080/08935696.2013.843250
Business Wire (2004) Cisco selected to build backbone and premium business network for China telecom's IP next generation network. *Business Wire*, 15 November. https://www.businesswireindia.com/cisco-selected-to-build-backbone-and-premium-business-network-for-china-telecom's-ip-next-generation-network-6171.html
Carsten P (2015) China drops leading tech brands for certain state purchases. *Reuters*, 27 February. https://www.reuters.com/article/us-china-tech-exclusive/china-drops-leading-tech-brands-for-certain-state-purchases-idUKKBN0LV08720150227
Cave D, Hoffman S, Joske A, Ryan F and Thomas E (2019) Mapping China's technology giants. *The Australian Strategic Policy Institute*. https://www.aspi.org.au/report/mapping-chinas-tech-giants
Center for Security and Emerging Technology (2020) *Original CSET translation of "Certain major issues for our national medium- to long-term economic and social development strategy"* [*国家中长期经济社会发展战略若干重大问题*], *Qiushi* [*求是*]. https://cset.georgetown.edu/wp-content/uploads/t0235_Qiushi_Xi_economy_EN.pdf
Chen Y (2021) Chinese AI dragon confronts fiery new realities. *Reuters*, 1 April. https://www.reuters.com/article/us-china-ai-breakingviews-idUSKBN2BO427
Chen J (2020a) Competition of AI four little dragons: Megvii's Hong Kong stockmarket breakthrough [AI四小龙"竞逐：旷视科技闯关港股]. *CB* [*中国经营报*], 1 November. http://hk.stock.hexun.com/2020-01-11/199930828.html
Chen L (2020b) U.S. blacklist hurt Megvii's sales before IPO attempt. *Bloomberg*, 7 April. https://www.bloomberg.com/news/articles/2020-04-06/u-s-blacklist-hurt-china-ai-giant-s-sales-ahead-of-ipo-attempt
Chen Q (2019) Huawei assured on 5G contracts. *Global Times Business*, 16 April. https://www.globaltimes.cn/content/1146179.shtml
Cisco (2004) *Cisco announces IP next-generation network advancements for service providers*. https://www.cisco.com/c/dam/global/en_uk/assets/news/pdfs/2004/20041206.pdf
Cisco (2008) *2008 Cisco corporate social responsibility report*. https://www.cisco.com/c/dam/assets/csr/pdf/CSR_Report_2008.pdf
Cohn C and York JC (2011) Eff urges Microsoft and Cisco to reconsider China. *EFF*, July. https://www.eff.org/deeplinks/2011/07/eff-urges-microsoft-and-cisco-to-reconsider-china
Creemers R (2017) Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China* 26(103): 85–100. https://doi.org/10.1080/10670564.2016.1206281
Dai S (2019a) Rising Chinese AI star Megvii gets caught in the US-China tech war. *South China Morning Post*, 29 May. https://www.scmp.com/tech/article/3012103/rising-chinese-ai-star-megvii-gets-caught-us-china-tech-war
Dai S (2019b) China facial recognition unicorn Megvii pledges to guard against weaponisation of AI on road to IPO. *South China Morning Post*, 26 August. https://www.scmp.com/tech/enterprises/article/3024395/china-facial-recognition-unicorn-megvii-pledges-guard-against
Department of Foreign Affairs and International Trade (1998) Canadian business deals in Beijing. *Bloomberg*, 24 November. https://www.bloomberg.com/press-releases/1998-11-23/canadian-business-deals-in-beijing
Fajgelbaum PD, Goldberg PK, Kennedy PJ and Khandelwal AK (2020) The return to protectionism. *The Quarterly Journal of Economics* 135(1): 1–55. https://doi.org/10.1093/qje/qjz036
Fan P (2006) Catching up through developing innovation capability: Evidence from China's telecom-equipment industry. *Technovation* 26(3): 359–368. https://doi.org/10.1016/j.technovation.2004.10.004
Forbes (2007) Cisco revs up China. *Forbes*, 1 November. https://www.forbes.com/2007/11/01/cisco-china-investments-markets-equity-cx_ml_1101markets17.html?sh=43e3cf8d4e74
Fortune (2020) *Huawei*. https://fortune.com/global500/2019/huawei-investment-holding/
Foster JB and McChesney RW (2014) Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review* 66(3): 1–33. https://doi.org/10.14452/MR-066-03-2014-07_1
Fouskas VK and Gökay B (2019) Global power-shift, the decline of the west and new authoritarianism. In Fouskas VK and Gökay B (eds) *The disintegration of euro-Atlanticism and new authoritarianism: Global power-shift*: 11–45. Cham: Springer International Publishing.
Franklin J and Zhu J (2019) Goldman evaluating role in China's Megvii IPO after U.S. blacklist. *Yahoo! News*, 9 October. https://yhoo.it/2YcHkBw
Galbraith J (2019) United States seeks extradition of Huawei official charged with violating sanctions against Iran. *American Journal of International Law* 113(2): 388–393. https://doi.org/10.1017/ajil.2019.14

Greenberg A (2009) Nortel's China syndrome. *Forbes*, 12 January. https://www.forbes.com/2009/01/11/nortel-huawei-buyout-tech-enter-cx_ag_0112nortel.html?sh=17155b032118
Griffiths J (2019) *The Great Firewall of China: How to build and control an alternative version of the internet*. London, UK: Zed Books Ltd.
Hamblen M (2004) Cisco drops lawsuit against Huawei. *Computerworld*, 28 July. https://www.computerworld.com/article/2566426/cisco-drops-lawsuit-against-huawei.html
Hickey AR (2008) Cisco denies aiding Chinese web censorship. *CRN*, 20 May. https://www.crn.com/news/networking/207801396/cisco-denies-aiding-chinese-web-censorship.htm
Huawei (2020) *Huawei investment and holding 2019 annual report*. https://www.huawei.com/au/annual-report/2019
Human Rights Watch (2019) *China's algorithms of repression: Reverse engineering a Xinjiang police mass surveillance app*. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass
Inkster N (2019) The Huawei affair and China's technology ambitions. *Survival* 61(1): 105–11. https://doi.org/10.1080/00396338.2019.1568041
Internet Data Center (2020) China's AI market. *Geren Tushuguan* [*个人图书馆*]. http://www.360doc.com/content/20/0521/02/5434130_913594072.shtml
Jaisal EK (2020) The US, China and Huawei debate on 5G telecom technology: Global apprehensions and the Indian scenario. *Open Political Science* 3(1): 66–72. https://doi.org/10.1515/openps-2020-0006
Jayasuriya K (2006) Beyond new imperialism: State and transnational regulatory governance in East Asia. In Hadiz VR (ed) *Empire and neoliberalism in Asia*: 31–51. New York, NY: Routledge.
Juego B (2018) Authoritarian neoliberalism: Its ideological antecedents and policy manifestations from Carl Schmitt's political economy of governance. *Halduskultuur*. 19(1): 105–36. https://doi.org/10.32994/ac.v19i1.209
Kaska K, Beckvard H, and Minarik T (2019) Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Center for Excellence.* https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/
Kehoe J (2014) How Chinese hacking felled telecommunication giant Nortel. *Financial Review*, 28 May. https://www.afr.com/technology/how-chinese-hacking-felled-telecommunication-giant-nortel-20140526-iux6a
Lai Stirland S (2008) Cisco leak: 'Great Firewall' of China was a chance to sell more routers. *Wired*, 20 May. https://bit.ly/3a7t5Un
Larson C (2018) China's AI imperative. *Science* 359(6376): 628–630. https://doi.org/10.1126/science.359.6376.628
Lasslett K, Green P, and Stańczak D (2015) The barbarism of indifference: Sabotage, resistance and state–corporate crime. *Theoretical Criminology* 19(4): 514–533. https://doi.org/10.1177/1362480614558866
Lim C (2020) Megvii technology mulling over possible IPO on Nasdaq-style star market. *Business Times*, 23 April. https://www.btimesonline.com/articles/130855/20200423/megvii-technology-mulling-over-possible-ipo-on-nasdaq-style-star-market.htm
Linneberg MS and Korsgaard S (2019) Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal* 19(3): 259–270. https://doi.org/10.1108/QRJ-12-2018-0012
Lyon D (2015) *Surveillance after Snowden*. Oxford: Polity Press.
M2 Presswire (2009) Nortel: China businesses cite need for improved security and management in data center survey; Identity-aware networking and centralized voice and data management hold the key. *M2 Presswire*, 10 December. https://www.m2.com/m2/web/story.php/2009C443EEECC07AF7A68025765E00643A51
MacKinnon R (2011) Liberation technology: China's networked authoritarianism. *Journal of Democracy* 22(2): 32–46. https://doi.org/10.1353/jod.2011.0033.
Marx, GT (2018) High policing. In Bruinsma G and Weisburd D (eds) *Encyclopedia of criminology and criminal justice*. New York, NY: Springer. https://doi.org/10.1007/978-1-4614-5690-2_460
Mills A, Durepos G, and Wiebe E (2012) Qualitative analysis in case study. In Mills A, Durepos G, and Wiebe E (eds) *Encyclopedia of case study research*: 749–757. Thousand Oaks, CA: SAGE.
McMorrow R (2019) Huawei a key beneficiary of China subsidies that US wants ended. *Phys*, 30 May. https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html
Megvii (2020) *About us*. https://megvii.com/en
Murakami Wood D (2017) The global turn to authoritarianism and after. *Surveillance & Society* 15(3/4): 357-70. https://doi.org/10.24908/ss.v15i3/4.6835
Nathan A (2015) China's challenge. *Journal of Democracy*, 26(1): 156–170. https://doi.org/10.1353/jod.2015.0012
O'Reilly C (2010) The transnational security consultancy industry: A case of state-corporate symbiosis. *Theoretical Criminology*, 14(2): 183–210. https://doi.org/10.1177/1362480609355702

O'Reilly C and Ellison G (2006) 'Eye spy private high': Re-conceptualizing high policing theory. *The British Journal of Criminology* 46(4): 641–660. https://doi.org/10.1093/bjc/azi090
Pei M (2018) China in Xi's "new era": A play for global leadership. *Journal of Democracy* 29(2): 37–51. https://doi.org/10.1353/jod.2018.0023
ResponseSource (1998) *Nortel Networks signs contract valued at over US$120 million*. https://pressreleases.responsesource.com/news/1834/nortel-networks-signs-contracts-valued-at-over-us-120-million/
Saunders B, Sim J, Kingstone T, Baker S, Waterfield J, Bartlam B, Burroughs H, and Jinks C (2018) Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity* 52(4): 1893–1907. https://doi.org/10.1007/s11135-017-0574-8
SFRC Democratic Staff (2020) The new big brother: China and digital authoritarianism. *United States Senate*. https://www.foreign.senate.gov/download/2020-sfrc-minority-report_-the-new-big-brother---china-and-digital-authoritarianism
Shen Q (2019) Goldman evaluating role in China's Megvii IPO after US blacklist. *CNBC*, 8 October. https://www.cnbc.com/2019/10/09/goldman-evaluating-role-in-chinas-megvii-ipo-after-us-blacklist.html
Shu C (2019) Megvii, the Chinese startup unicorn known for facial recognition tech, files to go public in Hong Kong. *TechCrunch*, 26 August. https://techcrunch.com/2019/08/26/megvii-the-chinese-startup-unicorn-known-for-facial-recognition-tech-files-to-go-public-in-hong-kong/
So AY (2019) The rise of authoritarianism in China in the early 21st century. *International Review of Modern Sociology* 45(1): 49–70. https://repository.ust.hk/ir/Record/1783.1-103392
Sun Y (2018) Innovators under 35: Entrepreneurs. *MIT Technology Review*. https://www.technologyreview.com/innovators-under-35/2018/
The Canadian Encyclopedia (2018) *Nortel*. https://www.thecanadianencyclopedia.ca/en/article/nortel
Tombs S (2012) State-corporate symbiosis in the production of crime and harm. *State Crime Journal* 1(2): 17–195. https://doi.org/10.2307/41937906
Tsinghua University (2018) *On the capacity of triply selective MIMO fading channels.* http://www.sist.tsinghua.edu.cn/publish/sist/11686/2018/20181024095530859891847/20181024095530859891847_.html
U.S.–China Economic and Security Review Commission (2011) *The national security implications of investments and products from the People's Republic of China in the telecommunications sector*. https://www.uscc.gov/research/national-security-implications-investments-and-products-peoples-republic-china
Udemans C (2020) Megvii's open-source platform offers Chinese AI alternative. *TechNode*, 25 March. https://technode.com/2020/03/25/megviis-open-source-platform-offers-chinese-ai-alternative/
Uhlmann C and Grigg A (2018) Secret meeting led to the international effort to stop China's cyber espionage. *Financial Review*, 13 December. https://www.afr.com/world/asia/secret-meeting-led-to-the-international-effort-to-stop-chinas-cyber-espionage-20181213-h192ky
Vitaliev D (2008) Corporate complicity with the Great Firewall. *The Guardian*, 13 August. https://www.theguardian.com/commentisfree/2008/aug/13/china.censorship
Walton G (2001) *China's Golden Shield: Corporations and the development of surveillance technology in the People's Republic of China*. Montreal, QC: International Centre for Human Rights and Democratic. https://catalogue.nla.gov.au/Record/2050094
Wood DM (2017) The global turn to authoritarianism and after. *Surveillance & Society* 15(3/4): 357–370. https://doi.org/10.24908/ss.v15i3/4.6835
Xu X (2021) To Repress or to co-opt? Authoritarian control in the age of digital surveillance. *American Journal of Political Science* 65(2): 309–325. https://doi.org/10.1111/ajps.12514
Yin RK (2018) *Case study research and applications: Design and methods*. Los Angeles, CA: SAGE.
Yu H (2017) Motivation behind China's "One Belt, One Road" initiatives and establishment of the Asian Infrastructure Investment Bank. *Journal of Contemporary China* 26(105): 353–368. https://doi.org/10.1080/10670564.2016.1245894
Zhang Y (2019) Made in China: New opportunities [中国制造"墙里墙外"都要香]. *Communication Information News* [*通信信息报*], 3 March. http://www.txxxb.com/yc/yc/2019/0311/207991.shtml