ABSTRACT

Scholars and policymakers have been increasingly concerned about technological competition between China and the United States over the past decade – made worse in recent months amid broader disagreements on global trade and the handling of the Covid-19 outbreak. Efforts by Washington and Beijing to promote the development of several dual-use technologies including 5G, artificial intelligence and quantum computing have become a core aspect of their strategic competition.[2] Yet understanding what constitutes a "strategic" industry is critically important for both theoretical purposes as well as policymaking. Focusing on nuclear technology and the market for cybersecurity products – viewed as strategic priorities – in United States and China, this paper outlines the variables that shape government decisions to intervene via trade policy and investment rules in these markets.

Market-oriented efficiency does not adequately explain state-firm relations and its broader impact for civilian and military applications of dual-use technologies. Trade and investment measures designed to protect strategic industries and maintain a security of supply are emblematic of the need to shift the analysis of the global economy. Hitherto, economic analysts have focused on efficiency gains and the reduction of transaction costs rather than considering the political and strategic aspects of trade and capital flows. Several governments – potentially pushed by the current crisis – would be expected to continue to use economic levers to compete in high- and low-technology sectors. For net exporters of intellectual property such as the United States and European countries, there may be significant impact resulting from the rise of alternative (and potentially cheaper) sources of advanced technologies. Moreover, with continued aggressive state intervention, China will challenge Western technological dominance with attendant security implications.

KEYWORDS

Strategic trade, cybersecurity, technology, dual-use technology, nuclear, US-China relations, state intervention.

[2] For our purposes, "dual use" refers to technologies with both civilian and military applications.

CONTENTS

1. INTRODUCTION

Much of the academic literature on dual-use technologies remains atheoretical and fails to examine the causes and consequences of state intervention in technology markets as an example of broader trends in the global political economy. Rather, analysts have focused on single-technology sectors – failing to see the forest for the trees and leaving an understanding of what constitutes a strategic technology unexplained.

Following the Covid-19 pandemic, analyzing what constitutes a strategic industry is important for both theory and policymaking. As *The Economist* recently noted, the key question facing policymakers is which economic activities have strategic consequences for the state – with the attendant risk of all economic activities being designated as important for international security (Economist 2020).

To some extent, this conundrum reflects a long-held debate among economists. Neoliberal economists have generally focused on the goal of efficiency, while neomercantilists have emphasized "security of supply". To many neoliberal economists there is no conflict in this distinction. From a neoliberal economic perspective, seeking the lowest-cost global production is in fact the *solution* to security of supply. However, supply chains following the logic of efficiency have led to excessive reliance on bottlenecks – including in China – for both raw materials and manufactured goods. The shortage of masks and ventilators tied to Covid-19, as well as microchips and other building blocks of high-tech markets, serve as recent examples contributing to a rethinking of efficiency as the central goal of economic policy.

A neomercantilist emphasis on the danger of efficiency at the cost of security of supply, however, comes with its own problems. Firms have long had an interest in portraying their industry as being "strategic" so as to secure protection, subsidies and other types of state intervention to restrict competition. For example, in the aftermath of the 2008 financial crisis, state responses went beyond at the border and traditional behind the border protectionist measures to what was aptly labeled "murky protectionism" (Baldwin and Evenett 2009; Aggarwal and Evenett 2010; Aggarwal and Evenett 2013). The determinants of these interventions, however, remain under-explored.

In this paper, we set out a conceptual framework to examine the factors that drive state intervention in national economies. In the process, we outline the various trade and investment-related interventions – both at and behind the border – that states use to influence markets that they view as strategic priorities. In Section 2, we review the existing literature concerning dual-use technologies and the government's role in supporting research and development efforts. Section 3 defines four mutually exclusive types of state intervention in domestic technology markets. Section 4 outlines the variables that shape government decisions to intervene in these markets. In Section 5, we consider these

variables across two countries – the United States and China – and two technology sectors; nuclear technology and the market for cybersecurity products. Finally, Section 6 outlines the future applications of this conceptual framework to address questions regarding the causes and consequences of state competition in emerging technology markets as well as its consequences for broader US-China strategic competition.

2. DUAL-USE TECHNOLOGIES AND STRATEGIC INTERVENTION

This section examines the existing literature concerning government intervention in domestic markets for dual-use technologies. We argue that the best way to conceptualize dual-use technologies is on a continuum.

Technologies rarely have purely civilian or military applications and as a result are distributed on a continuum. Some academics, particularly constructivists, argue that a technology's placement on the continuum represents a social construct.[3] While ideational concerns are present, this treatment ignores the material factors – whether technological, structural or economic – that define the dual-use potential of technologies. It is these factors that explain how and when technologies that were previously thought of purely in civilian terms (for example, personal protective equipment) become strategically important. As the importance of dual-use technologies rise, incentives for state intervention increase – as we have seen in 2020 in the markets for ventilators, gloves and masks.

In the existing literature exploring dual-use technologies, much of the discussion has focused on how to prevent the spread (or proliferation) of specific technologies – nuclear, chemical or biological (Tucker 2012). Consequently, much of the literature has explored the use of regulatory and legal means to create export control regimes or international treaties to address specific concerns. The Nuclear Suppliers Group (NSG), Missile Technology Control Regime (MTCR), Australia Group (AG) and the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) serve as attempts to address the proliferation of technologies with dual-use potential.

Beyond the modal analysis of export control, others have explored the determinants of trade in dual-use goods (Fuhrmann, 2008). This analysis has tended to focus on technology flows at the state level despite the fact that private firms are often the relevant actors involved in technology transfer via joint-venture vehicles, selling goods to foreign markets and conducting cross-national research and development.

[3] For more on the process of "securitization", see: Buzan et al. 1998.

What both literatures above have in common is that they tend to focus on the exogenous effects of dual-use technologies: regime creation or technology spread. What these analyses miss, however, are the determinants of dual-use technologies themselves despite the long track record of state support for their development. Indeed, the dual-use nature of certain technologies often produces incentives for state intervention in those markets. Given the implications for energy diversification and efficiency, and the development of nuclear weapons, nuclear technology represents a salient example of this dynamic. Like other industries such as biotechnology and advanced computing, many states actively support their domestic nuclear energy markets. Crucially, pressures which produce the trend toward increased state support vary across several dimensions. Differences between these pressures offer a framework for understanding the processes of state support and the likely international consequences of such patterns.

3. STATE INTERVENTION AS A DEPENDENT VARIABLE

This paper focuses on the drivers of state intervention in technology markets rather than any type of state intervention *per se*. Several scholars have pointed to various types of state intervention in national markets that have effects on the global economy including economic sanctions, tariffs, quotas, subsidies and various industrial policies (Nolan 2001; Warwick 2013; Gereffi and Sturgeon 2013, 329; Cheung 2013; Carliner 1995, 21-32). Rather than treat each of these individually, this paper outlines two types of trade and investment policies – at the border and behind the border – that encapsulate interventions that are both collectively exhaustive and mutually exclusive. It is important to note that the term "behind the border" can be confusing as it does not always reflect the trade and investment policies undertaken within a particular economy by government actions. Traditionally, scholars have focused on the impact of behind-the-border trade and investment policies as they relate to imports. This paper argues that behind-the-border trade and investment policies not only affect import markets but also the competitiveness of a state's exports.

Though a variety of actors including firms, local authorities and other types of sub-national entities have a role in various types of state intervention, this paper focuses on the determinants of *state* intervention by national governments.

3.1 TRADE POLICY

This paper points to two different types of trade policy worthy of analysis.

3.1.1 At the border

Trade policies at the border "discriminate against foreign goods, companies, workers and investors" (Baldwin and Evenett 2009). These can take a variety of forms including import-taxing tariffs which make domestic goods more competitive than their foreign counterparts. Governments might also tax exports if they want to keep specific types of goods inside the country. Quotas operate similarly in that they limit goods arriving in, or exported from, the country (usually in terms of monetary value). Customs regulations represent an additional border measure that adds friction to the trade process.

3.1.2 Behind the border

There are several behind-the-border measures that affect trade patterns. Often these are described as measures used to drive "backdoor protectionism" (Cimino-Isaacs and Zilinsky 2016; Aggarwal and Evenett 2017). The most obvious behind-the-border trade measure is a regulatory environment that can be manipulated to discriminate against a foreign good or service. Regulatory standards, whether binding or voluntary, have an impact on market access. For example, product-content requirements (also known as localization rules) are often used to limit foreign-market access. Relatedly, the government is also a customer and can influence trade patterns through procurement rules.

Finally, domestic-market trade subsidies are designed to make goods from the targeted industry cheaper than their foreign counterparts (Baldwin and Evenett 2009). This has the dual effect of making imports less attractive and goods for export cheaper.

3.2 INVESTMENT POLICY

Investment policy offers a second vehicle for states to intervene in their domestic markets. Again, the distinctions between investment policy "at the border" and "behind the border" are used to distinguish between various types of intervention.

3.2.1 At the border

The most obvious intervention at the border are rules concerning foreign direct investment. Governments might limit shareholding of a publicly held firm at a specific percentage or review foreign acquisitions of domestic firms based on national security considerations. For example, in the US, the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) to address mandatory filing requirements for investments involving foreign governments, as well as foreign investment in firms deemed to represent critical infrastructure (Aggarwal and Reddie 2019).

3.2.2 Behind the border

Governments also influence direct and indirect investment behind the border. Traditionally, this type of state behavior has been captured in the context of industrial policy (Aggarwal and Evenett 2012). In terms of direct investment, governments often involve themselves directly in specific sectors of the economy or create state-owned vehicles that operate on their behalf. As with trade rules designed to protect foreign firms, direct and indirect investment provide domestic firms with an advantage within the domestic market and in preparation of their goods and services for export. Governments may also identify specific firms in which to invest and regulate both within the home

country and abroad. This practice is particularly common in the defense sector in the US and Europe as firms are often limited in terms of the goods and services that they can provide abroad, narrowing their ability to achieve economies of scale.

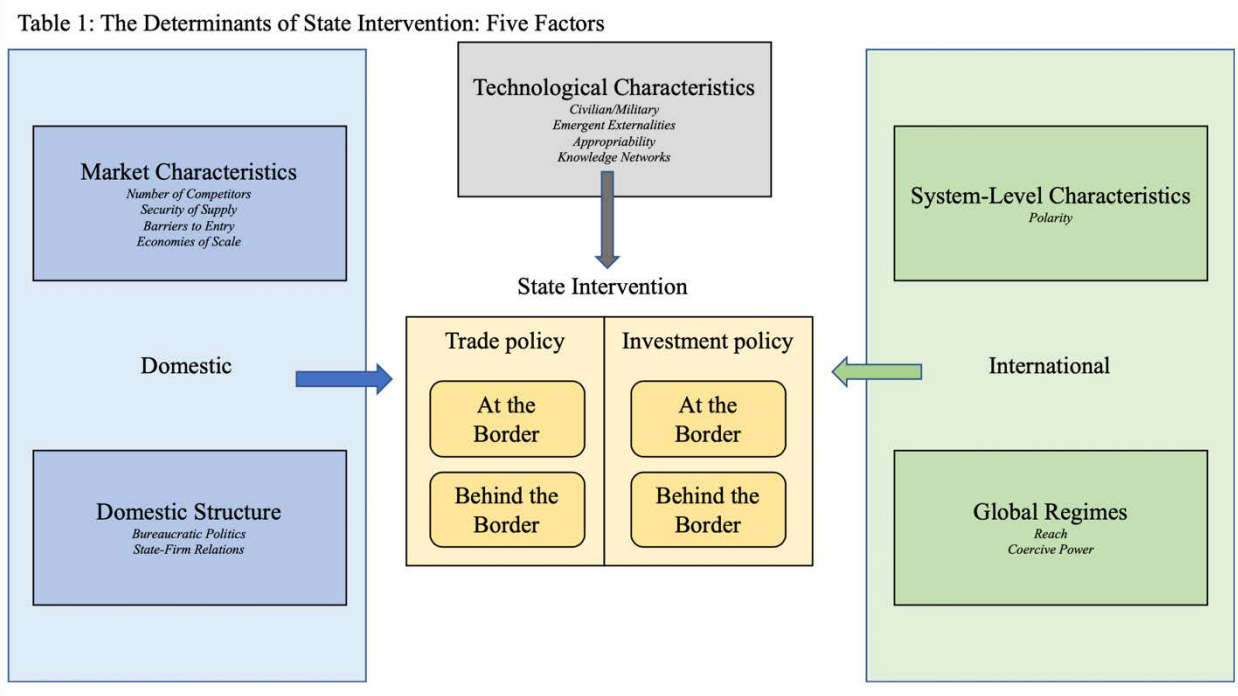
Governments also pursue indirect investment in strategic industries through human capital development programs. Indirect government interventions do not target a specific firm but rather identify a strategic need and subsidize the cost of creating knowledge networks necessary for the functioning of a particular industry.

This paper discusses state intervention in broad terms as an amalgam of the specific trade and investment measures above.

4. KEY FACTORS INFLUENCING STATE INTERVENTION

Having outlined the variety of ways in which governments intervene in their domestic markets, this paper argues that factors across five levels of analysis affect the type and magnitude of state intervention in markets for dual-use technologies. These five factors serve as the basis of a conceptual framework to examine the likelihood and character of government intervention to support the research and development of dual-use technologies.

Table 1: The Determinants of State Intervention: Five Factors



Below, we examine each of the five factors noted in Table 1. To be clear, we are not proposing an objective coding of what constitutes a strategic industry based on our estimate of its "true" dual-use nature. Rather, we specify variables theorized to influence whether policymakers will identify an industry as being strategic and then choose to intervene to bolster it in some way.

4.1 TECHNOLOGICAL CHARACTERISTICS

The technological characteristics associated with a particular technology affect whether a government intervenes in a technology industry as well as what types of intervention are deemed appropriate.

There are several characteristics of a given technology worthy of consideration. First, is a technology perceived as *primarily civilian* or *military* in nature? Some, such as nuclear

technology, have been viewed as primarily military and subsequently receive large amounts of direct investment and funding for research, development and deployment. The government is a primary customer of technologies under development in these markets.

Second, is the new technology likely to have *emergent externalities* for other industries or society as a whole? For example, fears regarding the effects of artificial intelligence (AI) on the future of work, provision of credit and patterns of surveillance have led to calls for government regulation of private firms developing AI technologies.

Third, is an emerging technology, its constituent components or precursors easily *appropriable*? Technologies that are simple to reverse engineer represent a challenge for state intervention as the easier they are to appropriate, the higher the chance that they may lead to technology transfer. Software, for example, is notoriously difficult to address using export-control mechanisms. At the same time, intervention may be considered less necessary when the technology in question is difficult to appropriate, leading to a hands-off approach. One of the forces driving the level of appropriation is the degree to which an emerging technology relies upon interdisciplinary knowledge networks. The breadth of human-capital requirements and knowledge networks that are necessary for research and development of emerging technologies vary and may also influence efforts by the state to invest directly in programs to address knowledge gaps.

Each of these characteristics offers a source of hypotheses regarding the likelihood or type of state intervention for further research. For example, technologies that have clear military applications and offer positive externalities for military ends are less likely to be appropriated by an adversary and require substantial investments in human capital—potentially increasing the likelihood of receiving government support. We engage with these hypotheses in the case study examining the development of nuclear and cybersecurity technologies in the US and China, respectively.

4.2 MARKET CHARACTERISTICS

Technologies do not exist in a vacuum. They are created by organizations often acting in the context of a market. This presents an important question: What dimensions of a specific industry are likely to influence state intervention? Several elements that Michael Porter analyzes and the industrial organization literature from which he draws upon are relevant to perceptions and decisions about state intervention (Porter 1979). While the number is potentially vast, given this paper's focus on dual-use technologies, our discussion centers on what we believe to be the four most important relevant variables: the number of competitors in the market, the diffusion of the supply chain, the barriers to entry, and economies of scale. We then discuss how variation in each factor is likely to affect the likelihood of government intervention.

The first variable we consider is the *number of competitors* in a given industry. As states evaluate the strategic importance of a particular industrial sector, we anticipate that sectors with fewer key players are likely to be seen as important for both national security and economic considerations. There are many examples of how this has played out in the US and elsewhere with burgeoning literature that has explored state supported "national champions" (Falck, Gollier, and Woessmann 2011).

From a national security perspective, firms in strategic industries have been subsidized and governments have been wary of foreign investment or takeovers of such firms given their small numbers. An example of this was the 2018 debate concerning the acquisition of Qualcomm by Broadcom (Westbrook 2018, 643). From a national economic focus, with the concept of "strategic" being stretched to include "societal resilience", governments have increasingly expressed a willingness to protect such firms against foreign takeovers (Lewis 2020). More directly, companies have been bailed out if they are perceived to be one of only a handful of players in a particular market.

A second key variable is supply resilience or *security of supply*. Efficiency is paramount for neoliberals, but the onset of Covid-19 alongside other global supply chain disturbances have increased concerns about the diffusion of supply chains and the consequences of relying on distribution networks with little slack to address crises. Even before the Covid-19 crisis, concerns about supply chains had been brought to the fore in the US with the election of Donald Trump and his appointment of Peter Navarro as a key adviser.

The title of an Interagency Task Force report from September 2018 was revealing: "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States" (Department of Defense 2018). The report warned that the US has a "surprising level of foreign dependence on competitor nations" and noted that "many sectors continue to move critical capabilities offshore in pursuit of competitive pricing and access to foreign markets." (Interagency Task Force 2018) The term "competitor nations" was primarily aimed at China. Thus, a key message of the report was that excessive supply-chain dependence on a single country, rather than a broader group of sources, will make governments more prone to engage in strategic intervention.

The literature on industrial organization has long emphasized the importance of a third market variable, *barriers to entry* (Bain 1950). This factor likely influences government choices pertaining to the labeling of an industry as strategic and therefore pursuing intervention. If barriers to entry for domestic and foreign firms are low in a given industry, there should be little incentive for the state to assist such firms from a security standpoint given the ease of access.

An interesting counter-example to this point is the apparel industry. Despite low barriers to entry, parts of this industry have long claimed to be of strategically important. Given the longstanding protection of the apparel industry from the mid-1950s to the mid-2000s, it is clear that in porous democratic states, bottom-up lobbying can lead to state intervention, even though from an objective standpoint, its strategic importance would be far-fetched (Aggarwal 1985). This points to the importance of looking at state intervention as an indicator of its actual importance for security, rather than as a measure of an industry's strategic nature. More generously, it could be argued that the large amount of employment generated by the apparel industry, while of little military value, provides rationale for protection.

The fourth variable is *economies of scale*. Industries such as aircraft production, auto production and steel production are significant economies of scale. Examples such as these are likely to be linked with the first variable, the *number of competitors*, as high economies of scale are likely to favor industry concentration. However, the presence or absence of economies of scale in various high-technology industries are likely to have an independent effect on decision-making on state intervention. States are tempted to intervene to protect industries with significant economies of scale as this allows firms in these industries to have lower production costs. For example, a defense industry's cost of production of fighter jets and bombers are highly dependent on the number of units that are produced, often leading states to promote foreign sales.

4.3 DOMESTIC STRUCTURE

The political-economy literature on industrial policy provides a platform for understanding the relevance of domestic governance arrangements for state intervention (Aggarwal and Aggarwal 2016). A key factor is the government's ability to resist *regulatory capture* by private firms. Academics have long distinguished between *strong versus weak* states (Katzenstein 1977, 879-920) arguing that the former are better able to resist lobbying efforts because of the nature of their bureaucracies and insulation from political pressures. The same literature also focuses on the extent to which societal groups are well organized.

Drawing on the work of policy analysts of East Asia industrial policy, Stephan Haggard argues that the strong state in both Taiwan and Korea and the "industrial organization and financial and corporate structure in both countries were directly influenced by the politics of business-government relations" (Haggard 2004, 72).[4] Additionally, Haggard noted that political elites in high-growth East Asian countries "enjoyed a degree of political, organizational and economic independence from the private-sector actors in the

[4] This section draws on Cheng 1990 and 1993, Fields 1995, and Noble 1998.

early phases of the region's growth, and this key political fact was reflected in institutional arrangements" (Ibid). Dani Rodrik also highlights the need to ensure a collaborative environment between governments and the private sector to reduce failures in state intervention. Examples of such collaboration include "deliberative councils, supplier development forums, investment advisory councils, sectoral round-tables or private-public venture funds" (Rodrik 2010).

Yet the debate about an "appropriate" political structure for successful state intervention continues. Even the widely accepted claim that corruption necessarily undermines intervention efforts has been challenged by David Kang (2002). At least conditionally, he argues that what distinguished South Korean success from the relative failure of government growth policies in the Philippines – in addition to the presence of an external threat – was the balance of power among business and government elites in Korea as opposed to the state-led domination of business in the Philippines. Thus, in Korea, both government elites and private firms found themselves in an iterated Prisoner's Dilemma game where cooperation for growth and intellectual property became possible.

When analyzing strategic-intervention decisions, a strong state is therefore more likely to succeed in resisting calls for industrial-policy protection. At the same time, coordination between well-organized societal groups cooperating with the state should also lead to more realistic intervention for strategic purposes. Examples of such coordination include South Korea and Singapore, both of which feature strong leadership by state bureaucrats in consultation with business groups. By contrast, weak states with well-organized lobbying groups are likely to intervene for reasons that have little basis beyond rent-seeking behavior.

4.4 GLOBAL REGIMES

In large part due to their *strength*, *geographical scope* and *issue scope*, international institutions are important influencers for the pursuit of strategic industrial policy. International institutions vary between those with global, overarching responsibilities such as the World Trade Organization (WTO) and those concerned with sectoral or regional/transregional arrangements. Regarding the former, sectoral agreements such as the 1996 Information Technology Agreement (expanded in scope in 2015) or the 1997 Basic Telecom Agreement (BTA) have provisions concerning tariffs, competition policy, licensing, regulatory independence and other policies that influence state intervention. On a transregional basis, the 11-member Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), concluded in 2018 after negotiations following the US withdrawal from the Trans-Pacific Partnership (TPP) in January 2017, contains provisions on standards and technical barriers to trade, investment, intellectual property and government procurement, among others. Regional agreements such as the North

American Free Trade Agreement (NAFTA), its successor the US-Mexico-Canada Agreement (USMCA), and the European Union (EU) contain a host of rules and regulations that influence what states are allowed to do.

Whether or not international agreements and institutions can genuinely *constrain state behavior* in practice remains and important question. Much has been written about the extent to which developing countries are constrained by the WTO in the pursuit of industrial policy by rich countries "kicking away the ladder" (Chang 2003). Critics have also argued that developed countries use protectionist measures to get to their place atop the pecking order, while simultaneously prohibiting developing countries from following them by "cement[ing] the head-start advantages of their firms through the WTO agreements" (Wade 2003, 633).

A recent study examined whether seven economies – the US, Russia, Japan, China, Brazil, the EU and South Korea – were complying with WTO rules when they intervened in the aftermath of the 2008 financial crisis (Aggarwal and Evenett 2012). In addition to observing significant variation in both discrimination against foreigners as well as domestic firms, the study found that countries varied in the degree to which they substituted classic trade measures with less regulated WTO rules such as "migration, bailouts and state aids, competitive devaluations, investment incentives, export taxes, trade finance, and steps by subnational governments and state-owned enterprises" (Ibid). The study concluded that this evidence "casts doubt on some of the strong claims in the industrial policy literature that WTO rules impose substantial constraints on government intervention, at least during the crisis era" (Ibid).

Historically, the WTO has been a critical factor constraining industrial policy. However, after confusion sparked by the Doha Round, the growing economic power of developing countries and the use of a variety of protectionist policies in the aftermath of the 2008 global financial crisis, recent evidence suggests that the WTO's role is increasingly shifting from *creating* to *interpreting* global regulation.

4.5 SYSTEMIC CHARACTERISTICS

A final key element influencing state intervention in strategic industries is the threat of global political environment variation, both across countries and time (Waltz 2000; Waltz 1979). *System polarity* represents a major structural characteristic of the international system worthy of consideration in driving state intervention in technology markets with dual-use applications.

For example, in a bipolar global political environment each of the pole powers will be in a competitive situation that may lead to a higher likelihood of pressure on state decisionmakers to intervene and bolster critical industries. By contrast, a unipolar global political environment with a single dominant power would pose the least risk. In the latter's

case, due to the strong position of the pole vis-à-vis potential peer competitors, there would be less pressure for state intervention to protect key industries. Further, in a multipolar global political environment, there may be less pressure from a security of supply perspective. In a multipolar world, however, there is potential that the highly competitive environment among states would lead to greater pressure for governments to intervene in support of their domestic markets.

5. ILLUSTRATIVE CASES: FROM NUCLEAR WEAPONS TO INTERNET TECHNOLOGY

We now explore the impact of the five factors across two illustrative cases in the US and China. Specifically, we examine the patterns of state intervention in the civilian nuclear and cybersecurity sectors in Beijing and Washington, respectively.

5.1 STATE INTERVENTION AND NUCLEAR TECHNOLOGY: FROM MILITARY TO CIVILIAN APPLICATIONS

Given its military consequences, role in civilian energy production, and latterly, medicine, nuclear technology is a clear example of dual-use technology. Following its creation with the Manhattan Project, nuclear technology has been the subject of discussions concerning nonproliferation of military uses, propagation of peaceful adoption and safeguards, and controls to ensure appropriate handling. Concerns surrounding nuclear materials developed "in concert with fears about the proliferation of nuclear weapons–related technologies in the early days of the Cold War, which included specialty steels, high-precision computer-aided manufacturing tools and facilities and high-performance software and hardware; that is, materials and tools that are readily adapted to nuclear weapons–related design and manufacturing" (Harris et al. 2016).

At the same time, there are considerable fears – renewed with the development of small, modular reactor designs in the past decade – that energy production might increase the risk of nuclear proliferation as several stages of the fuel cycle are potentially vulnerable to diversion of materials for weapons programs. Globally, the development of nuclear technology in both military and civilian applications have required cooperation and coordination between governments and private-sector actors, with some in the latter category often having close ties with the former.

In the sections below, we review the development of nuclear-technology markets in the US and China, paying attention to patterns of state intervention across each case and examining the impact of our five factors.

5.1.1 A nuclear market: The civilian nuclear sector in the United States

Government played a key role in tailoring the fissile material necessary for both contemporary military and civilian uses of nuclear technology. Administrations in the US, United Kingdom and Canada supported the "Development of Substitute Materials", known as the Manhattan Project, during World War II, leading to the first nuclear test in Alamogordo, New Mexico, and the first use of a nuclear weapon in August 1945.

The military operation was state-led but leveraged the capabilities of private firms during the war. In the immediate aftermath, attention turned to civilian applications of nuclear technology. The McMahon Atomic Energy Act in 1946 led to the creation of the United

States Atomic Energy Commission (AEC) to control nuclear energy development and peaceful uses of the technology. The regulatory role would be moved to Energy Research and Development Administration (ERDA), which would become the US Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC).

Through its "Atoms for Peace" program, the US government supported the nascent nuclear energy industry from its inception and financed the first commercial nuclear electricity plant in Shippingport, Pennsylvania. That plant attracted private-industry support to develop reactor technologies, with federal nuclear-energy programs shifting their focus to this area to support market creation for energy companies to engage with applications of nuclear technology.

The nuclear power industry grew rapidly in the 1960s as utility companies considered nuclear energy to be economical, clean and safe. During this time, the government played a regulatory role, while allowing energy companies to compete in the nuclear and broader energy sectors. Several private firms including General Electric and Westinghouse benefitted from early support of civilian nuclear technology in the US and continued to play a key role in its development and maintenance both domestically and abroad.

The importance of the international nuclear energy market for US firms increased significantly following a drop-off in investment in nuclear energy in the 1970s. Beginning in 2007, after nearly 30 years in which no new orders had been placed for nuclear power plants, a series of license applications prompted widespread speculation about a US "nuclear renaissance." (Vujić et al. 2012; Eaves 2017). The new license applications were driven by the improved performance of existing reactors, federal incentives from the Energy Policy Act of 2005, the possibility of carbon dioxide controls to increase costs at fossil fuel plants and volatile prices for natural gas.[5] However, despite recent advances in small, modular reactor designs and an increase in the number of small firms working on nuclear energy technology, the renaissance has been muted because of falling R&D funding.

Recognizing the early success of the US in generating nuclear energy, 31 countries began constructing power plants for commercial use – many contracting with American firms – even as US nuclear plant orders began to dwindle due to high capital costs, public concern about nuclear safety, and waste disposal and regulatory compliance issues. The transfer of nuclear technology has alarmed the United States, with initial concerns mainly for the proliferation of nuclear weapons as well as subsidiary use such as nuclear propulsion. These fears contributed to substantial efforts to create multilateral treaties

[5] Agreements for the first loan guarantees amounting to $6.5 billion for nuclear power plants under the Energy Policy Act of 2005 were signed February 20, 2014.

including the NPT and its associated safeguard regime, as well as a multilateral export-control regime, the Nuclear Suppliers Group (NSG).

The US also has its own collection of export control rules. The most important of these in the context of nuclear technology is Section 123 of the US Atomic Energy Act that requires bilateral nuclear-cooperation agreements prior to "significant transfers of nuclear material, equipment, or components from the United States to another nation". Following fears that Beijing was redirecting commercial nuclear technology toward military use, the US imposed new restrictions on commercial technology trade with China in 2018. American officials claimed that US-exported technologies were being diverted to power new generations of Chinese submarines, aircraft carriers and floating nuclear power plants (Sanger 2018). Relying on national security provisions, the trade restrictions introduced new tensions into the broader great-power competition over nuclear technology. Amid stringent regulatory requirements and with dwindling state backing of the civilian nuclear industry, private firms from other countries that enjoy government support – of which China is an example – out-competed American firms more often.

5.1.2 State support: Chinese direct investment in the civilian nuclear sector

As in the US, China's efforts in the 1950s to secure nuclear weapons technology were state-led. One of the major differences was that Beijing was not a first mover on nuclear weapons technology, but rather took advantage of advances made by the Soviet Union and used Soviet personnel, uranium and missile technology to build its nascent nuclear weapons program (Jersild 2013). With the government encouraging the rapid development and deployment of nuclear energy domestically and supporting exports abroad, Chinese state involvement in civilian nuclear technology has been robust in the years since its development of a nuclear weapon.

In 2000, China had only three commercial reactors compared to the 100 reactors in the US. As of 2020, China has 35 reactors with a further 20 under construction. The dramatic growth in the sector reflects government support for nuclear research and development programs to "promote core national interests, increase energy security, and reduce air pollution" (Ibid). President Xi Jinping declared in 2016 that it is the job of China's state-owned enterprises to support the enhancement of overall national power: "All Chinese nuclear entities are legally mandated to support China's security services" (Ford 2019). The civilian nuclear industry is reported to receive "direct support from China's civilian and military intelligence services, including from cyber espionage" (Ford 2020).

In contrast to the US export controls on civilian nuclear technology, Beijing has offered incentives to Chinese firms to export nuclear technology to foreign markets, despite

membership in the multilateral Nuclear Suppliers Group (Yellen 2020).[6] Since 2018, the Chinese government has put forward legislation supporting nuclear exports financially and technologically, including provisions calling for the convergence of military and civilian research on nuclear energy (Stanway 2018). China has adopted a build-own-operate (BOO) model under which the exporting nation handles everything from the financing and operation of a plant to waste management (Yellen 2020). China also includes human-capital development and direct state investment in nuclear exports (Banks 2017). While there have been few concerns that Beijing is not meeting its obligations under the Nuclear Suppliers Group multilateral export-control arrangement, China's willingness to export nuclear technology to Pakistan through its grandfathered nuclear commitments have drawn international scrutiny.

These developments reflect China's broader use of industrial policy to support strategic industries, operating a well-coordinated, top-down and goal-oriented approach aimed at closing the technological gap with the West. Domestic firms benefit from various forms of technology transfer, with foreign firms motivated to comply with Chinese requirements to gain access to its market and expand foreign business. This is particularly acute in China's civilian nuclear sector, given the decline in demand for nuclear power outside of China following the 2011 Fukushima disaster in Japan (Banks 2017). For example, Westinghouse's AP 1000 design has been used in four Chinese plants despite fears that cutting-edge commercial nuclear technology has been transferred as a result (Winning 2007). More recently, Bill Gates' TerraPower negotiated a contract in 2015 to build an advanced nuclear reactor in China. At the time, Gates noted that "there isn't the same budget that there was traditionally for doing experimental type reactors in the United States...Today, there's more experimentation to do in China than elsewhere." (LeVine 2016)

5.1.3 Reflections on the five factors in the nuclear case

There are similarities and differences across the five factors outlined above between China and the US, as well as variation in the degree of state intervention in the civilian nuclear sector. The *technological* characteristics, however, of civilian nuclear technology are similar in both cases. There are clear links to military applications, externalities for research and development efforts beyond the nuclear sector, a clear need for expertise across a large number of fields, and a technology that is appropriable but difficult to implement.

[6] See also: Thomas, Steve. "China's Nuclear Export Drive: Trojan Horse or Marshall Plan?" *Energy Policy,* 101 (2017): 683-691. It is important to note that China joined the Nuclear Suppliers Group in 2004 and currently follows its export control protocols.

Market conditions in the US and China differ considerably. In the US, civilian nuclear companies face competition in both the domestic and foreign markets. In China, the government limits and bounds competition. There are significant concerns about the security of supply of necessary precursors in both states. In the United States, the barriers to entry – driven by regulatory burdens and long approval processes – are high. In China, which has its own framework, the regulatory burden is lower. While neither civilian nuclear industries have achieved economies of scale, China appears closer to reaping the benefits of large-scale adoption.

Domestic structures across the two cases also vary widely, with state-firm relations closer in China than in the United States. Indeed, China's state-owned China National Nuclear Corporation has been supported domestically – and, over the past decade, internationally – by Beijing since its formation in 1955. On the other hand, early government support for the civilian nuclear sector in the United States has given way to a market-oriented approach leaving firms to largely fend for themselves in the global nuclear energy market. Some critics have argued that stringent export controls related to nuclear technology hamstring U.S. firms abroad (Fergusson and Kerr 2017).

Regarding *global regimes*, both states are members of overlapping international institutions designed to safeguard technology and prevent the proliferation of nuclear weapons. The reach and coercive power of these apparatuses – given the perceived importance of nuclear technology – are significant.

Finally, the international *system-level* characteristics differ between the United States and China. When the US was developing civilian nuclear technology, the conditions of the global nuclear-energy market shaped the decision of the US to adopt a market-oriented approach as it had a significant edge in both technological development and broader geopolitical power. Indeed, one might argue that Washington did not intervene in the US civilian nuclear sector because it did not need to. China, as a rising power, has had different imperatives – and the alternative approach to its civilian nuclear sector may reflect that position.

While these conclusions are not definitive, they suggest that variation in the five factors offer a useful platform for considering the drivers of state intervention in dual-use markets. Having outlined a case of dual-use technology that has its origins in military applications, we now turn to capabilities that have been dual-use from their inception.

5.2 INTERNET TECHNOLOGY AS A DUAL-USE TECHNOLOGY: THE CASE OF CYBERSECURITY

Unlike the nuclear case, internet technology has been more closely linked to civilian and economic applications rather than military applications. Indeed, it was ten years after the advent of the worldwide web that concepts such as cybersecurity, cyber defense and cyber offense came to the fore. That is not to say, however, that governments have not had a role in driving national cybersecurity markets (Aggarwal and Reddie 2018a). In the sections below, we examine state intervention in cybersecurity markets by the US and China. The analysis is complicated by the fact that competition between Washington and Beijing is, arguably, most salient in cyberspace.

5.2.1 The light footprint of a customer: Washington and cybersecurity

Beginning under the George W Bush administration, the US has emphasized cybersecurity to secure both government and private networks against cyber intrusions. To do this, Washington has employed a variety of policy tools including directly investing in firms working on cybersecurity applications, human capital development programs and using a series of at-the-border measures to punish those that it views as promulgating bad behavior.

US at-the-border policy measures have been a longstanding concern regarding Chinese firms – and more are being instituted as technological innovation and intellectual property grows in importance for cybersecurity (Lindsay, Cheung, and Reveron 2015). With numerous allegations characterizing China as an “advanced persistent threat” in cyber espionage, Washington is highly skeptical of foreign firms doing business in the US (Bejtlich 2015). A series of cyber-attacks emanating from China led to concerns of intellectual-property theft, technology transfers and the invocation of US national-security exceptions to the general conduct of international trade and investment. For example, the acquisition of 3Com by Huawei was prohibited by CFIUS in 2008 (Rogers 2012). Investigations of Huawei and ZTE in 2012 portrayed the companies as vehicles of the Chinese state and, subsequently, threats to US technology development (Ikenson 2017). These investigations led to US government procurement rules that prevented government agencies from buying Huawei and ZTE equipment. In recent months, this treatment has intensified with domestic firms prevented from selling chip design software to Huawei.

Historically, cybersecurity was primarily the concern of government and military officials. As the private sector is increasingly targeted by data breaches, as well as a source of cyber technology development, the defense community has recognized an imperative to expand its cyber strategy nationally. Consequently, Washington now relies on private cybersecurity firms and civilians to work on government cybersecurity and defense projects. Private-sector cyber defense firms offer network protection, intelligence

gathering and cyber-attack response capabilities for the government. While there are a variety of large cyber-defense contracting companies operating with different strategies and technological philosophies, such as CrowdStrike's "endpoint security," (CrowdStrike n.d.) they all have the capability of providing all-in-one cybersecurity services. For instance, CrowdStrike offers US government agencies the ability to secure devices, proactively monitor network traffic, block potential viruses and malware, secure vulnerabilities as well as respond to cyber-attacks and stopping them once they start.

Gigamon's public-sector offerings involve similar service capabilities, despite differences in the underlying technology and cybersecurity philosophy (Gigamon 2019). Federal agencies rely on private contractors to keep networks secure and functional. For example, the Department of Health and Human Services (HHS) has used Deloitte as a cybersecurity contractor from 2007 through 2019 (Criste 2019). When HHS suffered a cyber-attack in March 2020 during the Covid-19 crisis, the attack was unsuccessful (Stein and Jacobs 2020). While officials suspected the attack was state sponsored, HHS's cybersecurity infrastructure – and the contractors who manage it – successfully defended and protected the networks. Private cybersecurity companies have been effective, which explains their popularity among government agencies and the private sector (Waterman 2017).

However, private cybersecurity firms can be sources of weakness for government networks. For example, in 2015, vulnerabilities in the Office of Personnel Management's (OPM) cybersecurity contractor, KeyPoint, led to the leak of information of 22.1 million people (Nakashima 2015). KeyPoint was a small third-party contractor that focused on background checks for OPM and many other federal agencies (Boyd 2015). An earlier breach of KeyPoint's network systems allowed hackers to gain an access key to OPM's database and bypass security features that would have otherwise protected against a cyberattack (Boyd 2015). The issue could have been mitigated by the implementation of a mandatory two-factor authentication system, but without it, the attack went undetected (Fruhlinger 2020). The KeyPoint scenario illustrates a weakness that government cybersecurity contractors, rather than state-developed cyber-defense technologies, can pose for state information. If a cybersecurity firm has access to key resources, vulnerability inevitably exists for targeted cyberattacks and public information leakage.

Cybersecurity companies are not impervious to attacks themselves. For example, Amazon Web Services, which offers cybersecurity and cloud services for organizations and governments (Amazon Web Services 2020), was itself a hacking target in March 2020 that compromised sensitive information (Targett 2020).
Previous efforts to coordinate policies, strengthen internal defense systems and deter cyberattacks include the Computer Fraud and Abuse Act (CFAA) of 1986, the Financial

Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act, or GLBA), the Federal Information Security Management Act (FISMA) of 2002 and the Cybersecurity Information Sharing Act (CISA) of 2015 (Roche 1998; White House n.d.; White House 2009). Many of the threats identified in these laws pose a persistent vulnerability left unresolved, particularly as strategic dialogue has thus far focused on limited definitions of the technological application for deterrence outside the scope of civilian application. Early efforts including FISMA, passed under the administration of President George W Bush and updated in 2014, focused on providing cost-effective security to mitigate risks to the federal government, intra-agency protocols for security management, and system reviews (CSRC 2016).

Implemented in 2015 under the Obama administration, CISA sought to promote information sharing between the government and private sector and was an effort to mitigate private sector vulnerabilities due to the growing emphasis on private sector targets. The act allowed the Department of Homeland Security (DHS) to collect data on cyber threats and defensive capabilities from the private sector and protect firms providing information from potential liabilities (Heidenreich 2015). Due to ambiguity on information collection and usage of data, however, the act remains fraught with privacy risks and did little to support public and private sector collaboration. Further, CISA was thought to be complemented by the Protecting Cyber Networks Act, which would mitigate privacy concerns by forbidding firms to share data with the US National Security Agency (NSA) and the Department of Defense (DoD).

Though the Protecting Cyber Networks Act was passed in the house, it never cleared the Senate, leaving CISA to provide a framework for public-private information sharing (Tran 2016). Disagreements within and between government agencies and private firms drove the failure to create a cybersecurity regulatory regime. For example, private firms argue that they are best placed to define threats to cybersecurity and police their networks, fearing that burdensome cybersecurity regulations might arrest innovation. Consequently, they advocate for a light-footprint approach and have thus far been successful in these efforts. To some extent, the National Institute of Science and Technology (NIST) Framework – a non-binding information-sharing mechanism – serves as an example of the limited intervention of Washington to define the responsibilities of private firms to customers and competitors (Greer et al 2014).

5.2.2 Centralizing cybersecurity development in China

China's pursuit of defensive and offensive cyber capabilities involves an extensive range of strategic objectives and policy initiatives. These state interventions include industrial policy frameworks that promote state-led partnerships and emphasize technological self-sufficiency, sovereignty and leadership as well as directing military spending and managing the Digital Silk Road, an initiative designed to provide access to IT services to China's partners as part of the broader Belt and Road Initiative (BRI).

Since the founding of the People's Republic of China in 1949, five-year plans and other central government directives have been a consistent feature of policymaking. With regards to recent technological advances, the three most important initiatives are The National Medium- and Long-Term Program for Science and Technology Development 2006-2020 (MLP 2006-2020) (State Council of the PRC, 2006), Made in China 2025 (State Council of the PRC, 2015), and The 13th Five-Year National Plan for Science and Technology Innovation (13th Five-Year S&T Innovation Plan) (State Council of the PRC, 2016). In promulgating these plans, the State Council provided overarching objectives and general principles to guide policy support for a number of emerging technologies. All three initiatives assert the need for indigenous innovation and technological independence and leadership.

The term "indigenous innovation" (zizhu chuangxin, 自主创新) appeared 27 times in MLP 2006-2020 and 18 times in the 13th Five-Year S&T Innovation Plan. MLP 2006-2020 called for imported technology to be reduced to less than 30 percent of China's GDP by 2020 (State Council of the PRC, 2006). These plans also emphasized the development of dual-use technologies. For example, Made in China 2025 calls for innovation-driven development aimed at breakthroughs for key generic technologies in fields including digital, internet-based and intelligent manufacturing (State Council of the PRC, 2015). Such technologies include 5G, operating systems, software, robotics and aerospace equipment (State Council of the PRC, 2015). Furthermore, the 13th Five-Year S&T Innovation Plan calls for research and development of inter-city, intra-city and free-space quantum computing technology, a quantum-computing prototype and quantum simulator (State Council of the PRC, 2016), breakthroughs in machine intelligence based on big data analysis, human-machine fusion technologies and research on urban computing intelligence and system models (State Council of the PRC, 2016).

More broadly, the frameworks encourage state collaboration with, and support for, private companies. MLP 2006-2020 calls for science and technology policies to play a "guiding role" in an effort to make Chinese enterprises "the main structure for R&D investment" and "more rapidly perfect a unified, open, competitive, and orderly market environment" while also "leading enterprises to increase their R&D spending and promoting large

enterprises in particular to establish their own R&D structures through tax and financing polices" (State Council of the PRC, 2006).

It likewise describes a "national innovation system" (国家创新系统, guojia chuangxin xitong) that is "a social system with the government as the leading force that fully brings into play the foundational role of the market in resource allocation and in which various major innovative bodies are closely linked and effectively interact with one another" (State Council of the PRC, 2006). MLP 2006-2020, Made in China 2025, and the 13th Five-Year S&T Innovation Plan represent behind-the-border investment policies designed to shape the success of firms within Chinese government industrial policy emphasizing global leadership, self-sufficiency and public-private integration for dual-use technology innovation.

As overarching frameworks, these principles and efforts have implications for foreign affairs, both militarily and economically. Dual-use technologies also have implications for China's main infrastructure development strategy, the BRI, which has been defined as a "vast collection of development and investment initiatives [that] would stretch from East Asia to Europe, significantly expanding China's economic and political influence" (Chatzky and McBride 2020). Chapter 13 of the 13th Five-Year S&T Innovation Plan was titled "Building a 'Belt and Road' Collaborative Innovation Community."[7] The chapter calls for "close exchanges and communication with countries along the Belt and Road on science and technology policy" and "the formation of a cooperative network for science and technology innovation" (State Council of the PRC, 2016). In a speech on May 14, 2017, titled "Joining Hands in Promoting Construction of 'One Belt, One Road'",[8] President Xi Jinping declared,

> "We will persevere in the promotion and development of innovation; enhance cooperation in cutting-edge fields like the digital economy, artificial intelligence, nanotechnology, and quantum computing; and promote big data, cloud computing, and the construction of smart cities, linking together the Digital Silk Road of the 21st century. We will advance the deeper integration of technology industries and technology financing, optimizing the innovation environment and bringing together innovation resources. We will build innovation spaces and innovation workshops for young people of the internet age in a variety of countries, achieving the young dreams of the coming generation."[9]

[7] The original Chinese title is: "打造"一带一路"协同创新共同体"

[8] The speech is included in Xi Jinping's *The Governance of China, Volume 2* (《习近平谈治国理政》第二卷) as Chapter 16, "Promoting Cooperation on One Belt, One Road" (促进"一带一路"国际合作).

[9] Chinese translation: 我们要坚持创新驱动发展，加强在数字经济、人工智能、纳米技术、量子计算机等前沿领域合作，推动大数据、云计算、智慧城市建设，连接成 21 世纪的数字丝绸之路。我们要促进科技同产

Following the creation of the Digital Silk Road and with encouragement from the central government, Chinese tech companies have taken the lead on the sorts of technology extension Xi called for (Eurasia Group 2020, 6).

While these examples are illustrative rather than exhaustive, they speak to a range of activities potentially picking up speed along the Digital Silk Road creating conditions for Chinese firms to export their digital goods and services abroad while limiting competition domestically.

5.2.3 Reflections on the five factors in the internet technology case

Both Washington and Beijing have taken measures to address internet technology with different tools to varying degrees of success. China is currently developing a more stringent and centralized regulatory framework while the US is working through agency-specific initiatives. Though the US is using a "lighter touch" in its policies, China is leading with state controlled regulatory standards and data management. Beijing also appears to be more supportive of behind-the-border measures in Chinese firms, particularly regarding investment.

Unlike the nuclear case, internet technology has become a key component of the 21st century economy and civilian applications of it are often at the forefront of discussions. By virtue of representing a medium for commerce and communication, the internet has significant externalities for other sectors. Additionally, the technology is highly appropriable, particularly internet-related software. Cyber vulnerabilities also offer diminishing returns for those seeking to exploit them, creating a "use-it-or-lose-it" dynamic. Lastly, cybersecurity knowledge networks are disaggregated and there remain low-hanging fruit for attackers to leverage.

There are many competitors in the global cybersecurity market, particularly within the US. Among cybersecurity firms, there is considerable variation in size and services provided to customers which include government agencies, other firms and individuals. Given the low barriers to entry, the security of supply is high, though it is worth noting that cybersecurity firms rely on the networks that they seek to protect.

Domestically, the cybersecurity markets in the US and China vary considerably. The US has a disaggregated and weak regulatory architecture. China, on the other hand, has a centralized bureaucracy designed to govern the internal development of cyber capabilities and political apparatus that engages questions of cyber norms and governance abroad. Regarding state-firm relations, the US has continued to lobby for minimal state control. This is reflected in its regulatory architecture. In addition, while cybersecurity and the IT

业、科技同金融深度融合，优化创新环境，集聚创新资源。我们要为互联网时代的各国青年打造创业空间、创业工场，成就未来一代的青春梦想。

sector in the US is comprised of a large number of small firms often lobbying against government intervention, IT capabilities are more centralized in China with close ties between the state and firms.

Unlike nuclear technology, there are few international regimes addressing cybersecurity concerns. Discussions of international cyber norms are often relegated to several members of the United Nations Group of Governmental Experts (GGE) which has had minimal impact on state behavior. The relative positions of the US and China in terms of the distribution of their capabilities may also affect the government's conduct in their respective information economies. For a rising power, cyber capabilities might offer an avenue to engage in asymmetrical competition that holds an adversary's military capabilities at risk.

6. CONCLUSIONS

Is *laissez-faire* a lie? Whether in good or bad economic times, governments have consistently intervened to bolster what are perceived to be strategic industries. Both analysts and policymakers must seek to understand better the conditions under which governments intervene in the name of "security of supply" and label an industry as strategically important. Particularly in the security context of US-China technological competition, there is a danger that firms will lobby governments to simply seek handouts in the name of "security". As we have seen, intervention can come about as a result of lobbying by firms, while in other cases it has been driven by a top-down, government-led effort.

We have presented a conceptual framework to examine the factors that drive state intervention in dual-use technology industries. From our perspective, much of the existing literature emphasizes technological determinism that fails to examine the political economy imperatives associated with government intervention – from state-firm relations to bureaucratic politics. Although we argue that an industry's technological characteristics are worthy of examination, it is also important to understand an industry's market structure, a country's domestic structure, existing international regimes and the structure of the international system. Each of these elements, both by themselves and taken together, influence state intervention in high-technology industries.

How might this framework shed light on current US-China security competition? By focusing on nuclear technology and cybersecurity, we found that governments have been key actors in the research, development and deployment of both, and intervention tools used by each state vary. We submit that this activist approach to markets and industries viewed as "strategic" should move to other dual-use technologies. Moreover, there are significant differences in how states engage with their domestic markets – whether centralizing strategic objectives and direct investment behind the border or manipulating import and export markets through trade policy at the border.

Regarding nuclear technology, US policy has been reactionary, protectionist and fueled by proliferation concerns. By contrast, China's actions have been proactive in linking strategic military and economic interests. One example of this difference lies in US-China economic relations pertaining to nuclear technology transfer. As noted, the US has imposed several export controls on relations between its private firms and Chinese businesses which seek to leverage Western nuclear technologies.

For example, the US recently blocked its firms from dealing with China's General Nuclear Power Corp – a move which China described as a "misuse" of nuclear export-control standards (Stanway 2019). In a similar move, the US drafted laws meant to prevent Beijing from leveraging peaceful nuclear technologies for military applications—drawing

accusations from China of unfair and inappropriate national security linkages in economic arrangements (Davenport 2018). These examples illustrate the fraught nature of strategic linkages in economic agreements (Aggarwal 2013), with dual-use nuclear technology being a target for such arrangements.

Through the CFIUS, the US also placed import controls on nuclear-technology transfers, affecting foreign investment (Lovells, Desai, and Roma 2020). US officials have supported these types of controls on economic exchanges, with State Department representatives stating that Beijing "continues to seek advantage over foreign partners with little regard for bilateral agreements or other nations' laws" (Ford 2018).

Import controls have effectively hamstrung US nuclear development and has left market space for China and Russia to continue their nuclear "export-race" dominance, an issue which the Trump administration has been working to address (DiChristopher 2019). Some American analysts claim that permitting continued Chinese growth in this domain would introduce a welcome check on Russia's current dominance (Yellen 2020). The broader global reaction, however, remains strongly concerned with China's spotty record on export controls, as exemplified by its nuclear transfer relationships with Pakistan, Iran and other regions of geopolitical interest ("Chinese Nuclear Energy" 2020). US import controls and China's continued nuclear export growth are symbiotic, it is important to note.

IT markets feature similar dynamics, with Washington employing a lighter touch for regulation, procurement rules and export controls both at and behind the border. While Beijing has strict rules regarding joint ventures in return for market access, close state-firm relations and, arguably, a state apparatus to support technology transfer, the US has generally allowed its companies to operate transnationally, allowing foreign firms to partner with domestic industry unfettered by stringent regulation. That is not to say that Washington does not intervene, just that it does so with a lighter footprint through procurement rules, comparatively small investments and human capital development programs.

Under both the Obama and Trump administrations, Washington's position has shifted amid concerns that the access that Huawei, ZTE and Kaspersky Labs access have to the US cybersecurity market represents risks both to private firms and government agencies. These concerns have led the US government to alter its procurement rules and re-evaluate export-control and foreign-investment review processes. The question of how the US government should interact with private firms remains unresolved, given the strong ideological laissez-faire consensus (Aggarwal and Reddie 2018b).

The Chinese government is comparatively more interventionist in support of both its civilian nuclear and IT sectors. Beijing has used a variety of measures including trade policy, direct investment and technology transfer to bolster its domestic industries.

Technical, market and domestic characteristics often ignored by both economists and scholars of international relations appear to shape China's trade and investment policies.

Whether this argument holds across other technologies and countries is an open question. In future work, we intend to examine traditional dual-use technologies such as chemicals and biotechnology, as well as cutting-edge innovations including 5G, quantum computing and artificial intelligence. Future research may also seek to quantify the five factors in question to understand the broader implications of technology on strategic competition.

This argument demonstrates that market-oriented efficiency is inadequate to explain the variety of relationships between the government and private sector and the broader impact of these relationships for civilian and military applications of dual-use technologies.

Looking to the future, we will consider some key questions facing policymakers in the US, Europe and East Asia: Specifically, how might a shift in the future of high-technology products change as China becomes a net producer of intellectual property with dual-use applications? In light of the analysis on the five factors above, we argue that trade and investment policies in China and the US are likely to shift significantly.

Trade and investment measures designed to protect strategic industries and maintain a security of supply are emblematic of the need to shift our analysis of the global economy. Hitherto, economic analysts have focused on efficiency gains and the reduction of transaction costs rather than considering the political and strategic aspects of trade and capital flows. We expect several governments – potentially pushed by the current crisis – to continue to use economic levers to compete in high- and low-technology sectors.

For net exporters of intellectual property such as the US and countries in Europe, there may be a significant rise in alternative and potentially cheaper sources of advanced technologies. These developments may necessitate further foreign capital to service government debt as deficits increase. It remains unclear what this will look like, but several scholars have pointed to concerns that these shifts will dramatically alter the global economy for firms and governments.

One consequence may be the marrying of trade and investment policy with diplomacy, as Beijing has done. For example, China links development aid with trade in a manner that the US and Europe have eschewed over the past three decades. Put differently, Western firms compete to provide goods and services to the market. By contrast, though Chinese firms compete to provide goods and services, they also furnish ancillary benefits - whether financing, development aid, diplomatic ties or military assistance – both to the customer and to the country in which it is located. This affects North American and European firms that face growing competitive pressures in terms of market access and

more complicated and vulnerable supply chains as they are unable to secure similar levels of government support.

Recent legal and political developments in Hong Kong have highlighted the concerns that foreign firms engaged in high-technology R&D and finance have as they face questions surrounding their ability to conduct business in the Chinese special administrative region and consider whether to relocate or limit operations. How Hong Kong and conditions throughout the region alter the East Asian and global economies in the wake of Covid-19 remains to be seen.

Current developments yield many questions and few answers. What is clear is that economic orthodoxy, focusing on increasing efficiency and decreasing friction in the global marketplace, has failed to consider the requirements of governments around the world to balance systemic, market and technological imperatives.

BIBLIOGRAPHY

Aggarwal, Sonia N. and Vinod K. Aggarwal. 2016, "The Political Economy of Industrial Policy." *BASC Working Paper*, 16-01.

Aggarwal, Vinod K. 1985. *Liberal Protectionism: The International Politics of Organized Textile Trade*. University of California Press.

Aggarwal, Vinod K. 2013. "U.S. Free Trade Agreements and Linkages." *International Negotiation* 18, (1): 89–110.

Aggarwal, Vinod K., and Simon J. Evenett. 2010. "Financial Crisis, 'New' Industrial Policy, and the Bite of Multilateral Trade Rules." *Asian Economic Policy Review* 5, (2): 221–44.

Aggarwal, Vinod K., and Simon J. Evenett. 2012. "Industrial Policy Choice During the Crisis Era." *Oxford Review of Economic Policy* 28, (2): 261-283.

Aggarwal, Vinod K., and Simon J. Evenett. 2013. "A Fragmenting Global Economy: A Weakened WTO, Mega FTAs, and Murky Protectionism." *Swiss Political Science Review* 19, (4): 550–57.

Aggarwal, Vinod K., and Simon J. Evenett. 2017. "The Transatlantic Trade and Investment Partnership: Limits on Negotiating behind the Border Barriers." *Business and Politics* 19, (4): 549–72.

Aggarwal, Vinod K., and Andrew W. Reddie. 2018a. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." *Journal of Cyber Policy* 3, (3): 291–305.

Aggarwal, Vinod K., and Andrew W. Reddie. 2018b. "Comparative Industrial Policy and Cybersecurity: The US Case." *Journal of Cyber Policy* 3, (3): 445–66.

Aggarwal, Vinod K, and Andrew W. Reddie. 2019. "Regulators Join Tech Rivalry with National-Security Blocks on Cross-Border Investment." *Global Asia*.

Bain, Joseph. 1959. *Industrial Organization*. Hoboken: John Wiley & Sons.

Baldwin, Richard, and Simon Evenett. 2009. *The Collapse of Global Trade, Murky Protectionism and the Crisis: Recommendations for the G20*. CEPR.

Banks, George David. 2017. "The Rise of China's Civil Nuclear Program and Its Impact on U.S. National Interests." *American Council for Capital Formation Center for Policy Research,* (2017): 1-14. http://accf.org/wp-content/uploads/2017/03/ACCF_China_paper_03.pdf

Bejtlich, Richard. 2013. "China's 'Advanced Persistent Threat' to American Computer Networks." Hampton Roads International Security Quarterly 16 (July): 1-6.

Boyd, Aaron. 2015. "Contractor Breach Gave Hackers Keys to OPM Data." *Federal Times*, June 23, 2015. https://www.federaltimes.com/smr/opm-data-breach/2015/06/23/contractor-breach-gave-hackers-keys-to-opm-data/

Buzan, Barry, Ole Wæver, and Jaap De Wilde. 1998. *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Carliner, Geoffrey. 1995. "Industrial Policies for Emerging Industries." In *Strategic Trade Policy and the New International Economics*, edited by Paul Krugman, 21-32. Cambridge: MIT Press.

Chang, Ha-Joon. 2003. "Kicking Away the Ladder: An Unofficial History of Capitalism, Especially in Britain and the United States." *Challenge,* 45 (5): 63–97.

Chatzky, Andrew, and James McBride. 2020. “China's Massive Belt and Road Initiative.” *Council on Foreign Relations*, January 28, 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative

Cheng, Tun-jen. 1990. “Political Regimes and Development Strategies: South Korea and Taiwan.” In *Manufacturing Miracles: Patterns of Development in Latin America and East Asia*, edited by Gary Gereffi and Donald Wyman, 139-178. Princeton: Princeton University Press.

Cheng, Tun-jen. 1993. “Guarding the Commanding Heights: The State as Banker in Taiwan.” In *The Politics of Finance in Developing Countries*, edited by Stephan Haggard, Chung Lee, and Sylvia Maxfield, 55-92. Ithaca: Cornell University Press.

Cheung, Tai Ming. 2013. *Fortifying China: The Struggle to Build a Modern Defense Economy*. Ithaca: Cornell University Press.

Cimino-Isaacs, Cathleen, and Jan Zilinsky. 2016. "Local Content Requirement: Backdoor Protectionism Spreading under the Radar." *PIIE Trade and Investment Policy Watch*, July 22, 2016. https://www.piie.com/blogs/trade-investment-policy-watch/local-content-requirements-backdoor-protectionism-spreading

Criste, Laura. 2019. “HHS Recompetes $347 Million Cybersecurity Contract.” Bloomberg Government (blog). *Bloomberg Government,* April 17, 2019. https://about.bgov.com/news/hhs-recompetes-347-million-cybersecurity-contract/

CrowdStrike. n.d. “Protecting the Public Sector from Cyber Threats.” Security Solutions. https://www.crowdstrike.com/security-solutions/government-public-sector/

Davenport, Kelsey. 2018. "U.S. Restricts Nuclear Trade With China." *Arms Control Association,* November 2018. https://www.armscontrol.org/act/2018-11/news/us-restricts-nuclear-trade-china

Dean, Jeffrey, Greg Corrado, Rajat Monga, Kai Chen, Matthieu Devin, Mark Mao, Marc'aurelio Ranzato, et al. 2012. “Large Scale Distributed Deep Networks.” In *Advances in Neural Information Processing Systems* 25, edited by F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, 1223–1231. Mountain View: NIPS.

Department of Defense. 2018. "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States." *Interagency Task Force*, September 2018. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

DiChristopher, Tom. 2019. "The US is losing the nuclear energy export race to China and Russia. Here’s the Trump team’s plan to turn the tide." *CNBC,* March 21, 2019. https://www.cnbc.com/2019/03/21/trump-aims-to-beat-china-and-russia-in-nuclear-energy-export-race.html

Eaves, Elisabeth. 2017. "Can North America’s Advanced Nuclear Reactor Companies Help Save the Planet?" *Bulletin of the Atomic Scientists,* 73 (1): 27-37.

Eurasia Group. 2020. “The Digital Silk Road: Expanding China’s Digital Footprint.” *Eurasia Group*, April 8, 2020. https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf

Falck, Oliver, Christian Gollier, and Ludger Woessmann, 2011. *Industrial Policy for National Champions*. Cambridge: MIT Press.

Fergusson, Ian F., and Paul K. Kerr. "The US Export Control System and the Export Control Reform Initiative." *Congressional Research Service*, January 28, 2017. https://fas.org/sgp/crs/natsec/R41916.pdf

Fields, Karl. 1995. *Enterprise and the State in Korea and Taiwan*. Ithaca: Cornell University Press.

Ford, Christopher Ashley. 2018. "Chinese Technology Transfer Challenges to U.S. Export Control Policy." *United States Department of State*, July 11, 2018. https://www.state.gov/remarks-and-releases-bureau-of-international-security-and-nonproliferation/chinese-technology-transfer-challenges-to-u-s-export-control-policy/

Ford, Christopher Ashley. 2019. "Competitive Strategy vis-a-vis China: The Case Study of Civil-Nuclear Cooperation." *United States Department of State*, June 24, 2019. https://www.state.gov/competitive-strategy-vis-a-vis-china-the-case-study-of-civil-nuclear-cooperation/

Fuhrmann, Matthew. 2008. "Exporting Mass Destruction? The Determinants of Dual-Use Trade." *Journal of Peace Research* 45, no. 5 (2008): 663-52.

Gereffi, Gary, and Timothy Sturgeon. 2013. "Global value chain-oriented industrial policy: the role of emerging economies." In *Global Value Chains in a Changing World,* edited by Deborah K. Elms and Patrick Low, 329-360. Geneva: WTO Publications.

Greer, Christopher, David A. Wollman, Dean E. Prochaska, Paul A. Boynton, Jeffrey A. Mazer, Cuong T. Nguyen, Gerald J. FitzPatrick. 2014. "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0." *NIST Special Publication* 1108r3 (September): 1-246.

Haggard, Stephan. 2004. "Institutions and Growth in East Asia." *Studies in Comparative International Development* 38 (4): 53–81.

Harris, Elisa D., James M. Acton, and Herbert Lin. 2016. *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge: American Academy of Arts & Sciences.

Heidenreich, Brianna, and David H Gray. 2013. "Cyber-Security: The Threat of the Internet." *Global Security Studies* 4 (3): 1-10.

Ikenson, Daniel. 2017. "Cybersecurity or Protectionism? Defusing the Most Volatile Issue in the U.S.-China Relationship." *Cato Institute*, June 13, 2017. https://www.cato.org/publications/policy-analysis/cybersecurity-or-protectionism-defusing-most-volatile-issue-us-china

Interagency Task Force. 2018. "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States." *Interagency Task Force*, September 2018. https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

Jersild, Austin. 2013 "Sharing the Bomb among Friends: The Dilemmas of Sino-Soviet Strategic Cooperation." *Cold War International History Project*, Wilson Center. February 2019.

Kang, David C. 2002. *Crony Capitalism: Corruption and Development in South Korea and the Philippines*. New York: Cambridge University Press.
Katzenstein, Peter J. 1977. “Conclusion: Domestic Structures and Strategies of Foreign Economic Policy.” *International Organization* 31, no. 4 (1977): 879–920.
LeVine, Steve. 2016. "Bill Gates says China is the best place to pursue next-generation nuclear power". *Quartz*, March 1, 2016. https://qz.com/627113/bill-gates-says-china-is-the-best-place-to-pursue-next-generation-nuclear-power/
Lewis, Ted G. 2019. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. Hoboken: John Wiley & Sons.
Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron. 2015. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. New York: Oxford University Press.
Lovells, Hogan, Sachin Desai, and Amy Roma. 2020. "New CFIUS Rules Potentially Impacting Nuclear Foreign Investment." *JD Supra,* February 6, 2020. https://www.jdsupra.com/legalnews/new-cfius-rules-potentially-impacting-25646
Nakashima, Ellen. 2015. “Officials: Chinese had access to U.S. security clearance data for one year.” *The Washington Post*, June 19, 2015. https://www.washingtonpost.com/news/federal-eye/wp/2015/06/18/officials-chinese-had-access-to-u-s-security-clearance-data-for-one-year
NIST. 2016. “FISMA Implementation Project.” Accessed 3 May 2020. https://csrc.nist.gov/projects/risk-management/detailed-overview
Noble, Gregory. 1998. *Collective Action in East Asia: How Ruling Parties Shape Industrial Policy*. Ithaca: Cornell University Press.
Nolan, Peter. 2001. *China and the Global Economy: National Champions, Industrial Policy and the Big Business Revolution*. New York: Springer.
Nouwens, Meia and Helena Legarda. 2018. "China’s pursuit of advanced dual-use technologies." *The International Institute for Strategic Studies*, December 18, 2018. https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance
Office of the General Counsel. 1954. “Nuclear Regulatory Legislation.” *United States Nuclear Regulatory Commission*, 1954.
People’s Daily News. 2017. “Work Together to Promote the Construction of the ‘Belt and Road.’” *People’s Daily News*, May 14, 2017. http://theory.people.com.cn/n1/2018/0104/c416126-29746009.html
Porter, Michael E. 1979. “How Competitive Forces Shape Strategy.” *Harvard Business Review* 57 (1979) 137-145.
Roche, Edward M. 1998. "Critical Foundations: Protecting America’s Infrastructures." *Journal of Global Information Technology Management* 1 (1998): 49–50.
Rodrik, Dani. 2010. “The Return of Industrial Policy.” *Project Syndicate*, April 12, 2010. https://www.project-syndicate.org/commentary/the-return-of-industrial-policy?barrier=accesspaylog
Rogers, Michael and Dutch Ruppersberger. 2012. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies

Huawei and ZTE." *U.S. House of Representatives,* October 8, 2012. https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

Sanger, David E. 2018. "U.S. Puts New Restrictions on Nuclear Technology Exports to China." *The New York Times*, October 11, 2018. https://www.nytimes.com/2018/10/11/world/asia/us-china-nuclear-technology.html

Stanway, David. 2018. "China drafts new nuclear energy law, focus on international market." *Reuters*, September 22, 2018. https://www.reuters.com/article/us-china-nuclear-law-idUSKCN1M2024

Stanway, David. 2019. "China says U.S. block on nuclear firms a 'misuse' of export controls." *Reuters,* August 16, 2019. https://www.reuters.com/article/us-china-nuclearpower-usa-idUSKCN1V6005

State Council of the People's Republic of China. 2006. "Outline of the National Medium- and Long-Term Science and Technology Development Plan (2006-2020)" *State Council of the People 's Republic of China*, 2006. http://www.gov.cn/gongbao/content/2006/content_240244.htm

State Council of the People's Republic of China. 2015. "Notice of the State Council on Printing and Distributing "Made in China 2025" *State Council of the People's Republic of China*, May 8, 2015. http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm

State Council of the People's Republic of China. 2016. "State Council Notice on the Publication of the National 13th Five-Year Plan for S&T Innovation." *State Council of the People's Republic of China,* July 28, 2016. https://cset.georgetown.edu/wp-content/uploads/t0085_13th_5YP_tech_innovation_EN-1.pdf

The Economist. 2020. "Strategic Pile-up." *The Economist*, April 8, 2020. https://www.economist.com/business/2020/04/08/strategic-pile-up

The White House. 2003. "The National Strategy to Secure Cyberspace." *The White House*, February 2003. https://www.hsdl.org/?view&did=1040

The White House. 2009. "The Comprehensive National Cybersecurity Initiative." *The White House*, 2009. https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf

Thomas, Steve. "China's Nuclear Export Drive: Trojan Horse or Marshall Plan?" *Energy Policy* 101, (2017): 683-91.

Tran, Hiep, Enrique Campos-Nanez, Pavel Fomin, and James Wasek. 2016. "Cyber Resilience Recovery Model to Combat Zero-Day Malware Attacks." *Computers & Security* 61, (August 2016): 19–31.

Vujić, Jasmina, Ryan M. Bergmann, Radek Škoda, and Marija Miletić. 2012. "Small Modular Reactors: Simpler, Safer, Cheaper?" *Energy (Oxford)* 45, no. 1 (2012) 288-95.

Wade, Robert Hunter. 2003. "What Strategies Are Viable for Developing Countries Today? The World Trade Organization and the Shrinking of 'Development Space.'" *Review of International Political Economy* 10, no. 4 (2003): 621–44.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Reading: Addison-Wesley Publishing.
Waltz, Kenneth N. 2000. "Structural Realism After the Cold War." *International Security* 25, no. 1 (2000): 5-41.
Warwick, Ken. 2013. "Beyond Industrial Policy: Emerging Issues and New Trends", *OECD Science, Technology and Industry Policy Papers*, No. 2 (2003): 1-57.
Westbrook, Amy Deen. 2018. "Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions." *Marquette Law Review* 102, no. 3 (2019): 643-99.
Winning, David. 2007. "Westinghouse Seals China Deal." *The Wall Street Journal*, July 25, 2007. https://www.wsj.com/articles/SB118530110836876396
World Nuclear Association. 2020. “Nuclear Power in China.” *World Nuclear Association*, 2020. https://www.world-nuclear.org/information-library/country-profiles/countries-a-f/china-nuclear-power.aspx
Yellen, David. 2020. "The trade war we want China to win: China’s nuclear exports can challenge Russian dominance." *Atlantic Council*, February 26, 2020. https://www.atlanticcouncil.org/blogs/energysource/the-trade-war-we-want-china-to-win-chinas-nuclear-exports-can-challenge-russian-dominance/

ABOUT THE AUTHORS

Vinod K Aggarwal is Travers Family Senior Faculty Fellow and Professor in the Department of Political Science, and Affiliated Professor at the Haas School of Business, as well as director of the Berkeley Asia Pacific Economic Cooperation Study Center (BASC) at the University of California at Berkeley. He is editor-in-chief of the journal *Business and Politics.* With Sara A Newland, he is the editor of *Responding to China's Rise: US and EU Strategies,* published in 2014 by Springer.

Andrew Reddie is a postdoctoral fellow at the University of California, Berkeley where he serves as a researcher for the Berkeley APEC Study Center, Department of Nuclear Engineering, Goldman School of Public Policy, Center for Long-Term Cybersecurity and Carnegie-sponsored Project on Nuclear Gaming. He also serves as a Hans J Morgenthau Fellow, Bridging the Gap New Era Workshop Fellow, DoE Nuclear Science and Security Consortium Fellow, and Krulak Center Non-Resident Fellow at the Marine Corps University.

ABOUT THE ASIA GLOBAL INSTITUTE

Inaugurated on July 1, 2015, the Asia Global Institute is a multidisciplinary think tank co-established by The University of Hong Kong and the Fung Global Institute. Its mission is to generate and disseminate research and ideas on global issues from Asian perspectives.

DISCLAIMER

The views expressed in this report are those of the author and do not necessarily reflect those of the Asia Global Institute. The author is solely responsible for any errors or omissions.

ISSN: 2706-8554 (print), 2706-8552 (online)