Economic Drivers and the Reshaping of the International Security Landscape

Carol V. Evans

Introduction

Economic drivers are paramount in reshaping the global international security landscape. Military power as a determining factor shaping foreign policy influence has waned. Rather, nation states are increasingly employing economic instruments as a primary means of “projecting influence and conducting geopolitical combat in the twenty-first century.”

And, geostrategic competition itself is being determined by the degree to which a nation state uses these instruments effectively.

In this paper, I address three key economic drivers affecting geopolitics, with important implications for the international rules-based order and the security environment. The first economic driver is the rapid erosion of multilateral economic frameworks, hastened primarily by the focus of the administration of President Donald J. Trump on “America First” economic-nationalist policies. The Trump administration’s withdrawal from the Trans-Pacific Partnership (TPP), the renegotiation of the North American Free Trade Agreement (NAFTA), and the

1. For a thorough and absorbing discussion on geoeconomics, see Robert D. Blackwell and Jennifer M. Harris, War by Other Means: Geoeconomics and Statecraft (Cambridge: Harvard University Press, 2016), 33.
threat to withdraw from the World Trade Organization (WTO) presage a strong, preferential shift towards bilateral trade agreements. Ensuing trade wars with China and tariffs on strategic allies have had unintended consequences. These repercussive effects include stronger Sino-Russian relations, NATO disharmony, and countries from the Balkans to Southeast Asia being drawn into China’s economic orbit.

The second driver is the Belt and Road Initiative (BRI) embraced by President Xi Jinping of the People’s Republic of China. This $1 trillion infrastructure program involves an estimated eighty countries. Designed to secure China’s energy, natural resources, and trade routes in the maritime and overland environments, the BRI is enabling China’s ambitions of regional hegemony in the Indo-Pacific and may displace U.S. global power pre-eminence in the near future.

The third driver that affects international security is critical infrastructure (CI), which has now become the weapon of choice by nation states. Look no further than the Russian Federation’s hybrid operations in Ukraine and its cyber-attacks on the U.S. electric grid, as well as China’s strategic penetration of U.S. and European telecommunications, transportation, and defense industrial base sectors. These disturbing examples portend the capabilities and intentions of America’s adversaries to use critical infrastructure to shape the geostrategic battlespace and to undermine U.S. and NATO military supremacy.

**U.S. Retreat from Multilateralism**

Joseph Stiglitz, a Nobel Prize winning economist, suggested that when Donald J. Trump became president, he “threw a hand grenade into the global economic order.”2 Having based his election campaign on a promise to “Make America Great Again” by narrowing the U.S. trade deficit and creating jobs for American workers, Trump launched an economic nationalist agenda. This agenda astutely linked U.S. standing in the world with the need to wield geoeconomic might to ensure U.S. global military and economic competitiveness. The Trump administration also had a deep skepticism about the benefits of the multilateral world order that had largely been underpinned by U.S. and European leadership. Speaking in Brussels in December 2018, the Secretary of State, Mike Pompeo, announced that the international order “failed us,

---

and it failed you.” Pointing to the World Bank, the International Monetary Fund, and the WTO, Pompeo argued that “International bodies must help facilitate cooperation that bolsters the security and values of the free world, or they must be reformed or eliminated.”

The Administration’s “America First” approach marked what many economic observers consider to be a fundamental and dramatic shift in trade policy. Indeed, since 2017, the Trump administration used a range of geoeconomic tools—access to the U.S. market and the imposition of tariffs and economic sanctions—to reshape the global economic world order in America’s favor. It withdrew from the TPP; it renegotiated NAFTA; it threatened to withdraw from the WTO; and it encouraged the United Kingdom (UK) to leave the European Union (EU), i.e., “Brexit.” Certainly, these moves were indicative of President Trump’s aversion to multilateral and regional trade arrangements. As he put it in 2018, “Believe me, we’re going to have a lot of trade deals. But they’ll be one-on-one. There won’t be a whole big mash pot.” Instead, the administration’s focus has been on securing bilateral trade agreements with individual TPP members, South Korea (KORUS), Japan, and the UK, where the U.S. can exert greater leverage by virtue of America’s dominant economic and military positions. But one may ask at what cost?

One example of the negative repercussions for U.S. national security is the administration’s decision to exit the Trans-Pacific Partnership. The TPP was a signature trade policy of the administration of Barack

6. The U.S. has ratified free trade agreements with six of the TPP nations: Canada, Mexico, Peru, Chile, Australia, and Singapore, and is negotiating additional bilateral trade agreements with Japan and New Zealand. U.S. Trade Representative, “Trade Agreements,” https://ustr.gov/trade-agreements.
7. The TPP was a hotly debated issue in the 2016 U.S. presidential election. Democratic presidential candidates Hillary Rodham Clinton and Bernie Sanders both supported the U.S. withdrawal from the TPP, siding with the then Republican contender, Donald Trump.
Obama; it was designed to enhance U.S. leadership and commerce in the Asia-Pacific, and was seen as an important geoeconomic instrument supporting the U.S. “pivot to the Asia” strategy. As the then Secretary of Defense, Ashton Carter, affirmed in 2015, “passing TPP is as important to me as another aircraft carrier.” The U-turn in TPP policy by the Trump administration has had unintended consequences. American withdrawal has created a power vacuum in the region at a vital time when U.S. “activism” is needed to counter both China’s rising military presence in the Indo-Pacific and assertive economic hegemony via its Belt and Road Initiative. Absent U.S. leadership in promoting multilateral frameworks underpinning the global rules-based order, the Chinese president, Xi Jinping, has been quick to jump in and exploit this void by offering China’s own vision of a “community of common destiny for mankind” for the future of the international order, namely, Beijing’s long-term ambition to transform the international world order towards China’s authoritarian “governance model and emergence as a global leader.”

The Trump administration has stirred trade conflicts on many fronts with both adversaries and key allies, creating tension between the U.S. and NATO, and driving strategic partners further into the orbits of great-power adversaries: Turkey has been pushed into Russia’s orbit, while Italy, Greece, and the Philippines have gravitated toward China. While pushing Congress to ratify negotiated updates to NAFTA, the administration imposed duties on key Canadian and Mexican imports: 25 percent on steel and 10 percent on aluminum. These hit America’s NAFTA partners hard: In 2016, 88 percent of Canadian steel exports went to the U.S., and 73 percent of Mexico’s steel was exported to the U.S. Not surprisingly, Canada and Mexico immediately retaliated.

12. Canada retaliated by placing duties on $12 billion worth of U.S. exports, including whiskey and maple syrup, while Mexico slapped tariffs on $3 billion worth of American goods.
The administration also imposed steel and aluminum duties on Europe, South Korea, Japan, and India. These latter countries are key strategic partners and allies. Yet the rationale for the imposition of these tariffs was ironically on the grounds of national security to protect U.S. steel producers.13

Trade conflicts have also proliferated in the Indo-Pacific, and spread to India, the world’s largest democratic country, and a vital U.S. partner in the region. In June 2019 the administration terminated India’s designation as a beneficiary developing nation under the key Generalized System of Preference (GSP) trade program, after determining that India had not assured the United States that it would provide “equitable and reasonable access” to its markets.14 Continuation of GSP was a key element of Indo-U.S. negotiations on a bilateral trade package, which fell through in March 2019 when Washington announced its decision to end the GSP benefit. India has also faced potential secondary sanctions as part of U.S. pressure to reduce its imports of Iranian oil.15

India and the United States share many strong mutual interests in the region and avenues for military cooperation. These include countering China’s increasing naval encroachments in the Indian Ocean and monitoring Chinese economic and military activities with its northern nuclear rival, Pakistan, among many others. The fallout from these trade frictions has led New Delhi once again to question Washington’s reliability as a strategic partner.16

---

13. The Trump administration used Section 232 of the Trade Expansion Act of 1962 to restrict steel and aluminium imports because America’s armed forces and “critical industries” required a domestic supply of steel.


have observed, “Questions about trust, reliability, and motivations are deeply rooted, and perceptions that the United States eventually comes to dominate and even bully its strategic partners are real in New Delhi and beyond.”

Punitive U.S. economic sanctions on Russia, Iran, and Turkey have had additional unintended consequences for U.S. national security. For example, recent U.S. sanctions on Russian energy supplies have encouraged closer Sino-Russian cooperation in the energy and Arctic domains. U.S. sanctions against Iran, following America’s withdrawal from the Joint Comprehensive Plan of Action (Iran Nuclear Accord), spilled over to India and to Turkey, (both major importers of Iranian oil), straining the already fragile and important security relationships with these two countries. “We are not going to cut off our trade ties with Iran because other countries told us so,” responded the Turkish minister of economy, Nihat Zeybekci, by way of rebuke. In addition, the imposition of U.S. financial sanctions in 2018 against senior Turkish government officials over the detention of an American pastor has led to serious repercussions for the solidarity of the NATO alliance. These sanctions encouraged Turkey, an important NATO ally, to double down on its purchase of Russia’s S-400 air defense system, and for President Tayyip Erdoğan to pivot to Beijing to discuss infrastructure investment opportunities under the BRI.

**The Belt & Road Initiative: A Path to Global Pre-Eminence?**

Europe-Asia land bridge to form a greater Euro-Asian symbiotic economic belt and use the countless economic links and common interests with countries to the West in order to dismantle the U.S. encirclement of China.—PLA General Liu Yazhou

In September and October 2013, President Xi Jinping announced an

---


ambitious infrastructure development plan to build a “Silk Road Economic Belt” and a “Twenty-First Century Maritime Silk Road.” Originally called the One Belt One Road (OBOR) Initiative, in 2016, Beijing changed the name to the Belt and Road Initiative (BRI). The BRI is central to Xi’s larger vision of the “China Dream,” the great rejuvenation and restoration of the Chinese nation. The overland Silk Road economic “belt” entails six major infrastructure corridors intended to connect China’s underdeveloped western provinces to Europe through Central Asia via roads, bridges, high speed rail and telecommunication networks, pipelines, and other infrastructure. The maritime Silk Road consists of three blue-water economic passages: the China-Indian Ocean-Africa-Mediterranean passage, the China-Oceania-South Pacific passage and the China-Europe-Arctic Ocean route. Through massive investments in port infrastructure throughout the Maritime Silk Road (deep-sea ports and facilities, industrial free trade zones, energy storage and refining facilities, high-speed railways, etc.), China aims to secure sea lanes of communication (SLOCs) and trade routes for its energy, natural resource, and supply chain needs. Approximately eighty countries are participating in the estimated $1 trillion BRI, including countries from the Central Asian republics, the Middle East, South and South East Asia, Africa, the Caribbean, Eastern Europe, and most recently, Italy.

The BRI has attracted considerable interest and research by analysts, scholars, and policymakers in the past few years with proponents arguing whether the BRI is motivated more by Chinese geoeconomics or geopolitics—or both. Key economic drivers of the BRI include boosting the Chinese economy through spurring regional growth in China’s western provinces, particularly in Xinjiang; exporting chronic overcapacity in China’s State Owned Enterprises (SOEs) in the steel, cement, aluminum, and other construction related industries; stimulating demand for Chinese goods through the global expansion of exports and direct foreign investments by its SOE and private sector companies; promoting Chinese industry and technology standards in the energy, transportation and telecommunications sectors; and encouraging the

---

20. The six major overland corridors are the New Eurasia Land Bridge Economic Corridor, the China-Mongolia-Russia Economic Corridor, the Bangladesh-China-India-Myanmar Economic Corridor, the China-Central Asia-West Asia Economic Corridor, the China-Pakistan Economic Corridor, and the China-Indochina Peninsula Economic Corridor.
internationalization of the Chinese currency, the renminbi.\(^{21}\)

Other important economic factors shaping China’s BRI are its need to secure energy resources from neighboring Russia and Central Asia, Venezuela, and Brazil; as well as minerals and metals from Chile, Argentina, and Peru in Latin America, and Zimbabwe and the Democratic Republic of Congo in Africa.\(^{22}\) Concurrent to secure energy and natural resource supplies, is China’s goal to develop alternative maritime transportation routes to reduce dependence on the trans-shipment of these vital supplies from the Middle East via the Malacca Straits to China. Mitigating the so-called “Malacca Dilemma” is a top priority for Beijing as this artery is a strategic vulnerability since 80 percent of China’s oil imports, for example, pass through this narrow passage and the United States dominates this SLOC upon which China’s trade is reliant.\(^{23}\)

Speaking at the opening ceremony of the 2017 Belt and Road Forum, Xi promised that the BRI would help “foster a new type of international relations featuring win-win cooperation,” and that “exchange will replace estrangement, mutual learning will replace clashes, and coexistence will replace a sense of superiority.” He claimed that “in pursuing the Belt and Road Initiative, we will not resort to outdated geopolitical maneuvering.”\(^{24}\) Despite the rhetoric, one can well argue that the BRI is indeed a geopolitical platform from which to assert PRC’s influence with its neighbors. China has used BRI enticements to try to soften its strained relations with Japan, the Philippines, and Vietnam over its militarization of the Spratly Islands and the Paracel Islands and territori-

\(^{21}\) See Rolland, China’s Eurasian Century; Peter Cai, Understanding China’s Belt and Road Initiative (Sydney: Lowy Institute for International Policy, March 2017); Gal Luft, Silk Road 2.0: US Strategy toward China’s Belt and Road Initiative (Washington, DC: The Atlantic Council, 2017); Frankopan, New Silk Roads; CSIS website (National competing visions for connecting Asia), https://reconnectingasia.csis.org/analysis/competing-visions/.


\(^{24}\) Speech by H. E. Xi Jinping, President of the People’s Republic of China, At the Opening Ceremony of The Belt and Road Forum for International Cooperation (14 May 2017), http://www.xinhuanet.com/english/2017-05/14/c_136282982.htm.
al maritime disputes in the South China Sea, East China Sea, and the Sea of Japan.\textsuperscript{25} The geopolitical use of BRI incentives and controversial debt diplomacy tactics are also part of a deliberate strategy by China to coerce countries to break with Taiwan and to recognize Beijing’s “one China” policy.\textsuperscript{26}

Geoeconomics and geopolitics aside, China’s BRI “win-win” strategy hides more complex geostrategic ambitions. These ambitions, as in the Chinese game of “Go,” are subtly and intentionally posing major challenges to the United States and have the potential to alter the balance of power in the international system.\textsuperscript{27} Nowhere is this more evident than China’s calculated use of the BRI to establish global control of vital, strategic, maritime chokepoints, ports and sea lanes of communication, as part of a larger military transformation of China into a “maritime great power,” turning the People’s Liberation Army Navy (PLAN) into a “two-ocean navy” capable of confronting the U.S. Navy in the Indian and Pacific Oceans.\textsuperscript{28}

Let’s start with China’s control of key chokepoints under the BRI. Along the main China-Indian Ocean-Africa-Mediterranean passage, China has secured major, long-term port agreements with Cambodia, Indonesia, Malaysia, Brunei, Myanmar, Bangladesh, Sri Lanka, Pakistan, Djibouti, Tanzania, Namibia, Greece, and Italy. Djibouti is located roughly 250 miles from the Strait of Hormuz and on the choke point of Bab el-Bandeb, leading to the Red Sea and the Suez Canal. Half of the world’s containerized cargo passes through Djibouti, the only U.S. naval base in Africa and the primary base of operations for U.S. Africa Command in the Horn of Africa. Chinese berthing agreements in Malaysia, near the Straits of Malacca (the shortest route between the Indian and Pacific Oceans), and 99-year lease agreements for the deep


\textsuperscript{26.} Examples include the Dominican Republic, El Salvador, The Gambia, Panama, and the Democratic Republic of São Tomé and Príncipe.


water port in Gwadar, Pakistan, with proximity to the Persian Gulf, and the port of Hambantota in Sri Lanka in the Indian Ocean are other notable examples. Along the BRI’s China-Oceania-South Pacific route, China has made port acquisitions and other infrastructure investments in Australia, the Maldives, Vanuatu, Oceania, and the Solomon Islands.

Officially, Beijing maintains that these commercial ports are public goods, providing BRI countries with economic development, trade expansion, or helping to assist China’s U.N. anti-piracy, peacekeeping, and humanitarian missions. However, some China observers disagree with this benign characterization. They suggest that the PRC is using this global network of commercial ports as a precursor to the buildup of Chinese-controlled military logistics bases to counter U.S. naval dominance and to support future Chinese military operations. According to James Fanell, a former U.S. Navy Pacific Fleet intelligence officer, “The PRC is using state-owned companies and politically linked private firms to create a network of facilities designed to provide logistic support to deployed PLAN warships, employing a ‘first civilian, later military’ approach to port development across the region.”

The opaque, “civilian, later military” strategy is well evidenced in Djibouti, where the initial BRI commercial port agreement and development plan, generously funded through a $1 billion loan by Import-Export Bank of China, has morphed into a heavily fortified PLAN military base, with thousands of troops expected to deploy there. In recent testimony to the U.S. Congress, General Thomas Waldhauser, AFRICOM’s commanding officer, said that U.S. Africa Command “considers access to Djibouti and to critical global shipping lanes through the Bab-el-Mandeb strait an imperative to ensure U.S. strategic interests


are not compromised.”

Yet, that very access may be under threat as China could well leverage its hold on roughly 80 percent of the country’s debt to gain control over Djibouti’s ports.

The PRC strategy of debt trap control has also played out in the strategically located Sri Lankan port of Hambantota in the Indian Ocean. Struggling to pay its $8 billion debt to Chinese state-controlled BRI firms, Sri Lanka handed over the port of Hambantota to the China Merchant Ports Holdings Ltd. (CM Ports) on a 99-year lease. The Sri Lankan government’s decision to move a naval unit to Hambantota, and Beijing’s overtures to “gift” a frigate to the Sri Lankan Navy, creates opportunities for the insertion of PLAN training and support teams at Sri Lanka’s naval command, which is likely to encourage the positioning of additional Chinese naval assets at the facility. PLAN submarines and warships have already made unannounced port visits to Sri Lanka’s second port in Colombo, which is also majority Chinese-owned and operated.

There is also growing concern over Chinese BRI investments in the


Pakistani port of Gwadar. Geostrategically, Gwadar provides China with critical access to the Indian Ocean, without having to go through the Malacca Straits; it links China’s landlocked western provinces via the BRI China-Pakistan Economic Corridor. Pakistan owes China some $30 billion in BRI loans, and many analysts predict that China will leverage that debt as a means of ensuring the use Gwadar to expand and strengthen its maritime presence in the Indo-Pacific region, as a resupply base for the PLAN, and to service naval power projection in the Arabian sea.\textsuperscript{36}

Hambantota and Gwadar are but two crucial pieces of China’s BRI game of “Go” to form a network of important maritime access points—the so-called “String of Pearls” strategy—in the Indian Ocean. And while these two port developments pose immediate strategic challenges for India, naval strategist Alfred Mahan predicts that, “Whoever controls the Indian Ocean will dominate Asia, the destiny of the world will be decided on its waters.”\textsuperscript{37}

The impacts of China’s Belt and Road Initiative on the international security environment are enormous and wide ranging. First and foremost, the BRI is challenging U.S. military dominance in the Indo-Pacific region. Beijing’s use of ports for PLAN overseas based along the Maritime Silk Road, combined with likely deployments of the DF-26 anti-carrier ballistic missile system, will undoubtedly threaten U.S. force projection and sustainment capabilities and operations in the Korean Peninsula, Taiwan, and beyond. The BRI will be an effective mechanism to contain and deter India’s military reach on land and at sea. Whether China’s activities in the Indian Ocean will encourage the much needed “strategic convergence” between India and United States, as advocated by James Mattis, secretary of defense from 2017 to 2019, remains to be seen.\textsuperscript{38} Additionally, China’s future control of SLOCs threatens the energy and critical supply chains for forward deployed U.S. and NATO forces.

Despite these ongoing shifts in the tectonic plates underpinning the

\textsuperscript{36} Fanell, “Asia Rising.” In 2015 the PRC announced that it would sell eight submarines to Pakistan in a deal worth up to $6 billion.


\textsuperscript{38} Transcript of testimony by Secretary of Defense James Mattis before the U.S. Senate Armed Service Committee, “Political and Security Situation in Afghanistan,” 3 October 2017, \url{https://www.armed-services.senate.gov/imo/media/doc/17-82_10-03-17.pdf}. 
international balance of power, the U.S. and Europe, and by extension, NATO, have been surprisingly slow to recognize BRI’s impacts. The current U.S. administration has been focused on resolving its trade war with Beijing, Europe is fractured by Brexit, and by rising anti-EU movements in Italy, Germany, Poland, and Hungary. How the U.S. and Europe can devise a coherent strategy to counter China’s ascendance via the BRI in these circumstances remains unclear. Certainly the belated rebalance to the Indo-Pacific by the administration, and Washington’s promise of $113 million in new initiatives for the region are steps in the right direction. The Trump administration’s recent Blue Dot Network (BDN) initiative, with allies Japan and Australia, is the first major U.S.-led effort to redress the U.S.-China geoeconomic rivalry instigated by the BRI. The BDN is a welcome instrumental means to advantage the United States in its larger geostrategic competition with China and to signal its re-engagement in the Asia-Pacific region.

The Weaponization of Critical Infrastructure

A third economic driver reshaping the global international security landscape is the increasing use by Western adversaries of critical infrastructure (CI) as a weapon of choice. U.S. and NATO critical infrastructure, particularly the energy, transportation, information, communications, and the defense industrial base (DIB) sectors are being targeted as a potential means to disrupt logistics supply chains, and undermine military capability, readiness and force projection. As the 2017 National Security Strategy recognized, “The vulnerability of U.S. critical infrastructure to cyber, physical, and electromagnetic attacks means that adversaries could disrupt military command and control, banking and financial operations, the electrical grid, and means of communication.” In some cases adversaries are penetrating the critical infrastructure of


40. The U.S. Department of Homeland Security uses the USA PATRIOT Act of 2001 statutory definition of CI as “systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction…would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” See section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c (e)).

the U.S. and its allies to identify vulnerabilities for later exploitation. In many other cases, CI is being “weaponized” by Russia, China, Iran, and North Korea as part of their conduct of hybrid warfare.42

There are three domains where critical infrastructure is being used as a weapon and impacting international security in overt and more subtle ways. The first is the Russian Federation’s weaponization of CI in Ukraine, arguably as a testing ground for the development of larger hybrid warfare capabilities.43 The second is the penetration by Russia and other adversaries of the U.S. energy sector, particularly the U.S. electric grid, as a means of undermining future U.S. warfighting capabilities. The third is China’s strategic use of foreign investments to infiltrate and control key CI segments of the American and European defense industrial bases.

Hybrid Warfare in Ukraine

The linkage between CI as an instrument of hybrid warfare has been on open display in the Ukraine, where a Russian cyber army, closely affiliated with the Kremlin, has systematically attacked almost every sector of Ukraine’s infrastructure since 2014.44 Most notable were the attacks against Ukraine’s electric grid in December 2015, which left large parts of the capital city, Kyiv, and the western region of Ivano-Frankivsk in the dark, followed by another, more technologically sophisticated, attack in 2016 on one of Kyiv’s transmission substations. These attacks were set against the backdrop of Russia’s 2014 annexation of Crimea and continued military clashes in the eastern Donetsk and Luhansk regions in Ukraine.

Governments and cyber experts attribute these cyber-attacks to a Russian group known as Sandstorm, which deployed its BlackEnergy malware to penetrate specialized computer architectures that are used for remotely managing physical industrial equipment and control systems.45 What was most worrying to these cyber experts was that Sand-
storm, and another Russian-backed group called Energetic Bear, had already targeted NATO networks, and had compromised the computers of American and European electric and water utility companies with the same Trojan malware. This malware could provide these hackers with enough control to induce “blackouts on American soil at will.”

Reflecting at the time of the Ukraine electric grid attacks, one cyber forensic expert warned that “An adversary that had already targeted American energy utilities had crossed the line and taken down a power grid... It was an imminent threat to the United States.”

The repeated cyber-attacks against Ukraine’s CI as part of its hybrid warfare strategy serve Russian interests in several strategic ways. These attacks demonstrate the coercive power that Russia has exerted as part of its destabilization campaign against Ukraine. This campaign is designed to keep Ukraine in Russia’s continued orbit, by preventing Ukraine from reducing its energy dependence on Russia and thwarting Kyiv’s aims of integration with the European Union. Critical infrastructure, particularly in the energy realm, as a tool of Russian coercion, is certainly not lost on NATO and the EU. Since 2006 Russia’s Gazprom has repeatedly halted gas supplies in the midst of winter to Ukraine, a vital trans-shipment country with pipelines to Europe, over disputes on gas pricing. The upshot is that European countries, and NATO belatedly realize the vulnerabilities associated with their dependency on Russian gas supplies.

Another rationale for Russian CI attacks in Ukraine is to test, prove, and refine Moscow’s cyber warfare capabilities against a country that is unable to retaliate. In essence, use Ukraine as a test bed for Russian hybrid warfare in future global conflicts, which includes the United States. By turning the power off in Kyiv, Moscow is demonstrating

---

47. Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar.”
48. Europe could not survive thirty days without Russian gas in the winter; its vulnerabilities will only increase with Nord Stream coming online. Certain NATO countries, such as Germany, are more dependent on Russian energy supplies, leading President Trump at the 2018 NATO Summit in Brussels to tweet, “What good is NATO if Germany is paying Russia billions of dollars for gas and energy?”
49. Much attention has been paid to Russian influence operations and hacking activities during in the U.S. 2016 presidential election. For the purpose of this paper, the
to Washington its ability and willingness to weaponize CI to challenge America’s military might both at home and overseas.

**Russian Penetration of the U.S. Energy Sector**

In March 2018, the FBI and DHS confirmed that Russian government cyber hacker teams had actively “targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors.”\(^{50}\) The Russian cyber-attack teams included Sandstorm, Dragonfly, and Palmetto Fusion, with some attributed to gaining remote access to actual industrial control systems and U.S. energy sector networks, including a Kansas nuclear power facility.\(^{51}\) Cyber-attacks against the U.S. power grid have continued. The group Triton or Xenotime have compromised electric facility safety systems in order to cause potential plant disruption and damage. According to a researcher at the U.S. cybersecurity firm Dragos, surveillance of the U.S. electric grid is, “indicative of the preliminary actions required to set up for a future intrusion and potentially a future attack.”\(^{52}\)

Penetration of the U.S. electric grid has sounded alarm bells in the Pentagon. DoD installations and associated infrastructure depend on continuous and assured power to support military missions and operations both in the continental United States (CONUS) and outside contiguous U.S. (OCONUS).\(^{53}\) Any extended loss of power is what has been acknowledged as a glaring national security “Achilles heel.” The United States must expect adversaries to disrupt the flow of power, author would like to highlight the vulnerabilities to U.S. CONUS operations of Russian cyber penetration of America’s electric grid.


51. Greenberg, “Your Guide to Russia’s Infrastructure Hacking Teams.” This investigation led in part to U.S. Department of Treasury economic sanctions against five Russian entities and fifteen Russian individuals in March 2018.


53. Note that OCONUS does not refer to foreign countries but to the states and territories that are not part of the contiguous forty-eight states and the District of Columbia, i.e., Alaska, Hawai‘i, Puerto Rico, Guam, American Samoa, and the Northern Mariana Islands.
with cascading impacts on transportation, communications, and other CI services upon which the U.S. military depends. After all, for decades the former Soviet Union carefully studied the U.S. homeland and its warfighting infrastructure for infiltration and targeting purposes. The game-changing nature for today, however, is that with cyberspace, and the merging of CI with information and communications technologies, our adversaries no longer require kinetic solutions and direct military confrontation with the United States. Rather, as one senior DoD official conceded, “The smart thing to do is to maneuver around those forces, attack the critical infrastructure, the facilities here in the United States on which we depend to deploy, operate and sustain our forces abroad.”54 The use of CI by our adversaries as a means of hybrid warfare has larger international security implications and threatens true U.S. deterrence, for: “It does not matter how capable, how well trained or how advanced a nation’s forces are if they can’t get to the front in time.”55

Chinese Foreign Direct Investment in Western Industrial Bases

China, in particular, has made it a national goal to acquire foreign technologies to advance its economy and to modernize its military...It is comprehensively targeting advanced U.S. technologies and the people, the information, businesses and research institutions that underpin them.—Kari A. Bingen, U.S. Deputy Under-secretary of Defense for Intelligence.56

To achieve this national goal, China has used an effective combination of industrial, trade, and investment policies. Initiated in 2015, Beijing’s “Made in China 2025” industrial policy directs Chinese technological

development in important dual use areas: artificial intelligence, quantum computing, robotics, aerospace, autonomous and new energy vehicles, communications, and other emerging industries. China analysts have largely focused on the PRC’s illicit means to acquire these technologies through espionage, cyber operations, evasion of U.S. export control restrictions, and through coercive intellectual property sharing requirements on foreign companies investing in the Chinese market. Less attention has been paid to Beijing’s “Go Out” strategy of promoting Chinese state-owned and private sector champions to invest overseas, particularly in the United States and Europe, in key defense industrial base sectors.57

This inattention changed dramatically with the recent bid by Huawei, a Chinese tech giant, to provide 5G information and communications technology (ICT) networks in the United States and Europe. The case of Huawei poses a number of concerns for the physical infrastructure security of the defense industrial base (DIB) in the U.S. and Europe. For example: Should the U.S. and Europe be dependent on China to provide a key dual-use DIB infrastructure? Will China control the world’s wireless and telecommunications backbone? What is the true nature of the relationship between Huawei, nominally a private sector company, and the government in Beijing? Will the PRC use 5G networks as a “Trojan horse” for commercial and military espionage purposes?

The response by the Trump administration to Huawei was swift and decisive. It banned Huawei from all federal contracts for telecommunications equipment and services, and U.S. government contractors are prohibited from doing business with Huawei as well.58 In December 2018, Huawei’s Chief Financial Officer, Meng Wanzhou, who is also the daughter of the company’s founder, Ren Zhengfei, was arrested in Canada at the request of the United States. The U.S. Department of Justice filed formal charges of fraud, obstruction of justice, and theft of trade secrets against Huawei in January 2019. In addition, the administra-

57. Outward foreign investments and acquisitions have been assisted by Beijing-backed investment vehicles, such as the China Investment Corporation, and massive sovereign wealth funds. See “The White House,” How China’s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World (White House Office of Trade and Manufacturing Policy, June 2018).
58. The 2019 National Defense Authorization Act (signed into law in August 2018), and April 2018, the Federal Communications Commission (FCC) proposed rule: “Protecting against National Security Threats to the Communications Supply Chain through FCC Programs.”
tion has exerted considerable pressure on its allies within the Five Eyes intelligence community to ban Huawei from their respective markets.

Concerned about the larger implications of Chinese investments and other adversarial activities involving the U.S. DIB infrastructure, the Trump administration issued Executive Order 13806, which mandated an assessment of and recommendations for strengthening the U.S. innovation, critical manufacturing, and supply chain resiliency for the DIB. That assessment concluded, “All facets of the manufacturing and defense industrial base are currently under threat, at a time when strategic competitors and revisionist powers appear to be growing in strength and capability.” 59 In addition, the administration expanded the powers of the Committee on Foreign Investment in the United States, an interagency committee in the U.S. Department of the Treasury that reviews the national security implications of foreign investments.

European countries have been slow to recognize the potential security vulnerabilities and dependencies created by Chinese investments under the BRI in defense-related infrastructure. China has launched the 17+1 Initiative, a BRI forum which includes 12 EU member states and five Balkan countries, with major infrastructure loans going toward the construction of high-speed rail networks, port infrastructure, communications, bridges and highways. Chinese companies have acquired shipping terminals in Spain, Italy and Belgium. Major Chinese port infrastructure projects include the Italian ports of Trieste, Venice, and Ravenna, as well as the ports of Piraeus in Greece, Capodistria in Slovenia, and Fiume in Croatia.

Chinese involvement in key infrastructure projects in Europe (particularly in southern Europe and the Balkans), has garnered increasing concern by NATO regarding Beijing’s intentions. A recent NATO report emphasized the potential consequences for European security: “The degree and impact of foreign direct investment in strategic sectors—such as airports, sea ports, energy production and distribution, or telecoms—in some Allied nations raises questions about whether access and control over such infrastructure can be maintained, particularly in a crisis when it would be required to support the military.” 60

issues of energy dependency, NATO is grappling with dependency on host country infrastructure and the vulnerabilities this poses for logistics, secure communications, and other requirements to enable mobilization, force projection, and sustainment.

Chinese BRI investments in Europe are part of a deliberate strategy by Beijing to target the economically weaker EU NATO members to draw them into China’s economic orbit. Indeed, this strategy appears to be having some success. Hungary and Greece sought to block any direct reference to China in an EU statement regarding the ruling by the Permanent Court of Arbitration in The Hague that struck down the PRC’s legal claims in the South China Sea.61 Sounding the alarm over the long-term implications of European BRI investments on EU unity, Germany’s foreign minister forewarned, “If we do not succeed for example in developing a single strategy towards China, then China will succeed in dividing Europe.”62 The fact that Italy formally joined the BRI in March 2019 further highlights the failure of the EU to provide a counterbalance and comprehensive strategic approach to Chinese use of investments in defense critical infrastructure to undermine European economic security, upon which the NATO alliance relies.

A Changing International Order? Implications for the Security Environment

This chapter has identified three major economic drivers that are altering the topography of the international rules-based order, with varying implications for the security environment. With the erosion of the multilateral world economic order, caused in large part by the Trump administration’s “America First” economic policies, it remains to be seen what will be the full, long-term impact on the global security landscape. The retreat of U.S. leadership over the continued functioning of the rules-based order has created an enormous vacuum—one that China appears carefully maneuvering to fill. The Trump administration’s use of aggressive trade, investment, and other geoeconomic tools have been at the behest of national security objectives, punishing adversaries but straining relations with important allies and strategic partners in

The second driver re-shaping the international order is China’s Belt and Road Initiative. Arguably the BRI may prove to be the most significant geostrategic strategy of the twenty-first strategy. As discussed above, the BRI as a geoeconomic tool is dramatically restructuring the international political economy in ways that have yet to be fully understood. The BRI is a brilliant and flexible strategic global framework. Outwardly, it ensures the continued economic growth of the Chinese economy and economic ascendance globally. At the subterranean level, it also provides a means for regional hegemony within Asia, and signals the U.S. and Europe of its near peer ambitions.

The use of critical infrastructure as a weapon by Western adversaries is an important economic driver that has received little attention in international security circles. As we have seen, CI can be used as an instrument of hybrid warfare among weaker states such as the Ukraine, and against superpowers such as the United States. Whether through the use of cyber-attacks against a country’s infrastructure, or more covertly through surveillance and penetration, or via acquisitions and direct foreign investment, targeting of CI enables our adversaries to shape and control vital DIB infrastructure upon which U.S. and NATO militaries rely.

Is the international order changing? Absolutely. The economic and security challenges arising from a weakened international rules-based order, an ascendant China, fragmentation in the U.S. and Europe are just emerging. The issue is how nation states will adjust to and manage these shifts in the international order. Unilaterally, as it would seem in the cases of both the United States and the United Kingdom? Or do solutions to these challenges require a more multilateral, collaborative approach as they are beyond any one country’s reach? As Secretary Mattis concluded in his letter of resignation in 2018, “While the US remains the indispensable nation in the free world, we cannot protect our interests or serve that role effectively without maintaining strong alliances and showing respect to those allies.”