The Political Economy of the US-China Cybersecurity Relations and Trade War Under the Trump Administration

Miftahul Huda

Universitas Muhammadiyah Yogyakarta
Email: miftahul.huda.psc19@mail.umy.ac.id

Faris Al-Fadhat

Universitas Muhammadiyah Yogyakarta
Email: farisalfadh@umy.ac.id

Abstract

This *article examines the cybersecurity relations between China and the US under the Trump administration. It explores the changes in the US cybersecurity policy in 2019, where the US government took a protectionist approach to ban the operation of China's software and hardware in the US, and how such a decision predisposes the trade war between the two countries, which President Trump previously started. Appling the political economy approach of the cybersecurity concept, this research argues that the protectionist cybersecurity policy by the Trump administration was driven by the US business interest followed by security concern to lead the global technological transformation, balance the international economy, and preserve the US citizen's big data. Such policy, nevertheless, has intensified the trade war between the US and China, specifically in the technology and big data sectors. This study contributes to the broader literature on cybersecurity that has been much discussed in recent years.*

Keywords: *Cybersecurity, Trump administration, Trade War, US-China relations*

Abstrak

Artikel ini mengkaji hubungan keamanan siber antara Cina dan AS di

bawah pemerintahan Presiden Trump. Artikel mengeksplorasi perubahan kebijakan keamanan siber AS pada tahun 2019, di mana pemerintah AS mengambil pendekatan proteksionis dengan melarang pengoperasian perangkat lunak dan perangkat keras Cina di pasr AS, dan bagaimana kebijakan tersebut berdampak pada perang dagang antara kedua negara. Menerapkan pendekatan ekonomi politik dari konsep keamanan siber, penelitian ini berargumen bahwa kebijakan proteksionisme keamanan siber AS didorong oleh kepentingan bisnis dan keamanan untuk tetap memimpin transformasi teknologi global, menyeimbangkan ekonomi internasional, dan menjaga keamanan Big Data warga AS. Kebijakan tersebut, meski demikian, turut meningkatkan eskalasi perang dagang antara AS dan China, khususnya di sektor teknologi dan big data. Studi ini berkontribusi pada literatur yang lebih luas tentang cybersecurity yang banyak berkembang dalam beberapa tahun terakhir.

Keywords: Cybersecurity, *Pemerintahan Trump, Perang Dagang, Hubungan US-Cina*

INTRODUCTION

The history of the internet and cybersecurity are connected. Moreover, it is not easy to separate the impact of international relations on internet development. The internet first appeared in the 1960s, at the end of the Cold War between the United States (US) and the Soviet Union. The two nations were competing with one another to create a quick information system to win the war (University System of Georgia, 2022). A universal computer network system that connects with one another using the standard Internet Protocol Suite is defined as interconnection-networking (Internet) (Naughton, 2016).

Within the internet system, among essential aspects is the process of collecting and computing data termed "big data." It is defined as data from people (social media), organizations (government, NGO, company data), and machine learning, or artificial intelligence that analyses data into the appropriate graph form. Whether used for business intelligence, state intelligence, or other types of data collection and analysis, big data has the potential to enhance

information. It provides the potential to be a source of information, at least theoretically, making it usable by any organization, authority, or criminal network (Zwitter, 2015).

In international relations discourse, the introduction of big data that can be analysed by scientists has become a concern. For example, in 2003, the terrorist organization Al Qaeda managed to recruit militants through social media. Joseph Nye explained that the internet, which contains big data, is also a part of cyberspace, which harms the state politics and security, such as cyberattacks on official government accounts and financial institutions; cyberterrorism; or efforts made by terrorist organizations to recruit members via the internet, as in the case of Al Qaeda; and the most dangerous is the possibility of cyberwar if superpower countries conduct internet activities accidentally with sentience (Nye, 2011).

Among the numerous trade policies adopted by many governments, the US surprisingly pulled itself from the principles of free trade in 2018 by raising import duties on Chinese goods, particularly in the technology sector. It is well known that the US has prohibited importing Chinese goods such as Huawei, ZTE (Williams, 2020)economic, and geopolitical power. Concerns over companies such as telecommunications equipment-maker Huawei and social-media platform TikTok are multidimensional and scarcely amenable to characterization in terms of discrete national security risks. This paper traces one aspect of the \"securitization\" of technology policy in U.S.-China relations. It seeks to identify and disaggregate the main challenges facing policymakers who are troubled by China's growing technological power as expressed through the actual or potential effects of Chinese technology companies doing business in the U.S. market. These concerns can be broadly categorized along (at least. Since Donald Trump took office as President of the US in January 2017, the future relationship between the US and China appears to be more uncertain. Unfortunately, as a result of President Trump's "America First" policy, the US has withdrawn from several international agreements, and Washington has a new strategy for conditionally participating in allied agreements in Europe and Asia, which reduces its credibility in the eyes of other countries. In addition, the Trump administration is inclined to face Beijing with a

mindset of all-out confrontation, which might worsen US-China rivalry and eventually triggering to a new Cold War (Arežina, 2019; Beitelman, 2020)

The Trump administration's plan for the US includes launching a trade war against China. For various reasons, Trump has repeatedly declared war on China since 2018, a year after he was sworn into office. Trump said that China benefited from this situation because of the 2008 financial crises in the US and Europe. Due to the globalization of the US and other western nations taking advantage of China's employment policies and the flexible regulations for the entry of investment, post-Cold War relations between the two nations are in a good stage. China's admittance into the WTO served as an indicator of its entry into the international political sphere. However, initially, it was the US that served as China's economic mentor (Sun, 2019).

In July 2020, The US government filed a case to US Supreme Court to stop TikTok from operating in the US (The White House, 2020). TikTok was accused of selling client data to the Chinese government, posing a national security risk to the United States. According to Al Jazeera, the blockage of TikTok was one of the consequences of the trade war between China and the United States (Sukri, 2020). This research focuses on the changes in the US cybersecurity policy under the Trump administration toward China and how such a protectionist approach impacts the trade war between the two countries. This article argues that the protectionist cybersecurity policy by the Trump administration was driven by the US economic interests and social security concern. This is to steer the technological transformation globally, maintain economic stability, and protect the US citizens' big data for longer term. However, this strategy has exacerbated the trade conflict between the US and China, particularly in the technology and big data sector and industry. This study adds to the larger body of research on cybersecurity, which has received a lot of attention lately.

Theoretical framework and research method

The Conception of Cybersecurity

Before the 1970s, the world was familiar with the famous term "cybernetic" in 1948, when the Second World War broke out. This explanation of cybernetics is the study of messages to control machines and society. However, what

is discussed here is only a makeshift password computing system that has not been connected to other computing devices (Chotimah, 2019). The term "cybersecurity" was firstly introduced by computer scholars in the 1990s to describe the insecurity of the internet network, but it has since expanded from this technical issue to accommodate all internet activities that have become a threat to society as a whole. The lesson is when the internet network is used for terrorist purposes, as happened in 2001 when the WTC building was destroyed by terrorist planes using activities to threaten the country (Hansen & Nissenbaum, 2009).

Cyber securitization is extremely effective because it consists of a dual transfer of the political realm: from politicized to securitized; from political to technological. It requires an interdisciplinary effort to analyse and possibly combat the ramifications of the move. Since cyber security consists of several fields, it is crucial that analysis and academic discourse be applied to it. For example, the technological foundations of cyber security require that international relations scholars gain (Hansen & Nissenbaum, 2009; Lacy & Prince, 2018).

The desire to make technology safe to use—to decrease the number of potential harms—also contributes to cybersecurity. Cybersecurity is also concerned with the creation of secure, transparent, and managed goods, as well as the development of dependable and safe ICT behaviours and the establishment of relevant regulatory frameworks. Because people are the weakest role in the security chain and the final "consumers" of ICT services and infrastructure, any security solution must address social concerns (Mendhurwar & Mishra, 2021). On the other hand, security measures should not make the internet and information technology overly regulated, as this could seriously impact fundamental human rights. IT security connects with the legal, social, economic, and political sectors. It must not only represent its location as determined by the country, as well as that nation's values, culture, and civilization, but it must also meet the specific security requirements of the local environment (Ghernaouti, 2013).

Cybersecurity issues such as cyber espionage, cyber-attacks, hacktivism, internet control, and even technical problems such as internet neutrality are making headlines across the globe.

Cyberspace has evolved into a contentious political space shaped by competing interests, norms, and values. Diplomats (States) cannot remain silent as a result of this politicization. If cyberspace is only used for technical discussions among IT professionals, that era has come to an end (Barrinha & Renard, 2017).

Many aspects of security in the digital age are captured by liberalism: the multitude of non-state entities with transnational capability; network economics; "vulnerability interdependence," and the resulting perforation of officially sovereign borders. In strategic studies, realism philosophy is prevalent, and information warfare is fundamental. In this view, information warfare is the technical continuation of traditional kinds of psychological warfare and, more recently, electronic warfare. However, even from this angle, the analysis is still quite militaristic and state-centric (Eriksson & Giacomello, 2006).

A possible threat from digital and computerized technology is cybersecurity in international relations. It was further clarified that the security being discussed here is the same as national security in general, borrowing the term that national security is defined as having three key elements: first, the identification of "national" as a "state;" second, the assumption that the threat originates from outside the state's borders; and third, the use of military force to counter these threats (Valeriano & Maness, 2018).

A major challenge for every nation is to have the capacity to thwart or repel an invasion (Kusnanto, 2003). According to Adam Segal, great cyber powers consist of four components: large or technologically advanced economies; public institutions that control the energy and innovation of the private sector; unconventional and somewhat elite military and intelligence agencies; and an appealing story to tell about cyberspace (Segal, 2014).

Furthermore, cybersecurity has evolved into a vital component of national security. It refers to a state's capacity to defend itself and its institutions against dangers such as espionage, sabotage, crime and fraud, identity theft, and other harmful e-interactions and e-transactions. The most that can be done at this moment, in the lack of precedents, is to define the numerator (pressures) and monitor the denominator (capacity), to assess their relative behaviours through time. Any person or organization

can broadcast a message in most countries with internet access with the reasonable assumption that it won't be effectively — or at least not entirely — censored, controlled, or otherwise policed. Most of the time, the numerator is likely to be far more extensive than the denominator (Hansen & Nissenbaum, 2009).

Therefore, in this context of cybersecurity, the government approach and policy are likely to address the issue of national security and economic interests. The case of the US policy under Trump administration has mirrored this concern, where the expansion of China's technical product into the US market has endangered both trade and national security in the form of social big data. The US policy, hence, was a response towards such economic and security risk while pursuing the nation's interests in keeping its domination in technological industry globally vis a vis China's rise in this sector.

The Trade War Framework

The literature on trade wars in recent years has been dominated by the economic contestation between the US and China, specifically after the US under Trump started to take an extreme protectionist policy towards China's products and investments. Hence, the study on this topic has developed around the US-China trade war, trade policy, and trade theories. It is stated that the possibility of a trade war can affect other fields, such as geopolitical forces, markets, and the long-standing free market. Most countries around the world have adopted it (Qiu et al., 2019) if not longer. Many speculations about the reasons for and progress and potential implications of the trade war emerge. Countries must understand the reasons for the war to avoid future trade wars. Predicting what will happen in the near future and the related economic consequences are even more important for people (including businessmen and government policymakers.

We can categorize international trade into two phases: the first is traditional, and the second is modern. In the traditional phase, all countries still adhered to the protectionism school of trade until the theory of Adam Smith about free trade created liberalism. At the beginning of the emergence of the modern phase, economists began to propose a new theory, namely comparative advantage, to overcome the injustice of Adam Smith's free market. In the modern phase, the

fact is that there is an international organization appointed to be the arbiter of international trade, known as the WTO (Trend J. et al., 2020).

From a practical point of view, the three questions are interrelated and related. Why trade wars occur is a matter of international economics but is also related to international relations and politics. The former reflects the economic causes of trade wars, while the latter examines political interactions between countries and among various interest groups within a country. Looking at the international trade literature, theories on optimal tariffs, strategic trade policy, and cooperative and non-cooperative trade policy making have explained the interactive nature of trade policy making, including through extreme trade wars. Questions about how trade wars are conducted, why retaliation occurs, and what determines the outcome can be studied with the help of the useful analytical tools of game theory (Liang & Ding, 2020). Regarding the impact of trade wars, conventional trade theory explains well its price and welfare effects (Arežina, 2019)

In this research, we used a descriptive-qualitative method. The descriptive method aims to describe the facts of the policies and cooperation carried out by the Donald Trump Administration in related to cybersecurity in the US-China trade war. The research was conducted online and included a literature study. To avoid widening the explanation of the influence of cybersecurity in the trade war in the Trump administration, the author will limit the research time to 2018–2021.

RESULT AND EXPLANATION

The Origins of the Trade War

The US-China trade war is much more than just economic policy. It is part of the US political economic concern over its long-term supremacy in both economy and politics/security (Sahide, 2021). This is a very much shaped by the US global contestation and pressure from international major power, specifically with the rise of China in recent years. China's policy under Xi Jinping has been crucially marked by the capital expansion all over the continent, from Africa, Asia, Europe, to North America (Al-Fadhat & Prasetio, 2022). The massive expansion of China's economy through international trade, investment, and aid/loas has become a serious concern for the US government. Even before Trump launched a trade war with

China, the Obama administration explicitly identified China as a threat to the U.S. in high-end technology such as semiconductors and artificial intelligence as trade disputes increased in frequency and scale toward President Barack Obama's end years in office (Dupont, 2020). Due to national security, Trump launched a "Section 232 investigation" into importing steel and aluminium in June 2017. Given China's enormous capability for producing steel and aluminium, it is thought that the probe and the subsequently increased tax are directed toward China (Chong & Li, 2019).

Trade disputes between the US and China have become more frequent as 2018 progresses. The United States has imposed anti–dumping taxes, or tariffs, on Chinese imports since January 2018. Trade tensions increased after US President Donald Trump signed an executive memo to set up a "Section 301 investigation" into China's intellectual property practices and threatened to impose additional tariffs on Chinese goods (Chong & Li, 2019).

The US launched the trade war in response to three key concerns: (a) that China's persistently large trade imbalance was reducing job growth in the US; (b) that China was using illegal and unfair means to obtain US technology at a significantly reduced price; and (c) that China intended to undermine US national security and international standing. Given the history of disagreements that have accompanied China's path toward greater economic cooperation with the rest of the world, it is reasonable to assume that it will cause more problems (Liu & Woo, 2018)and they are (a.

US-China Tech War

The major goals of both the US and Chinese governments appear to be economic protectionism rather than cyber security (Ikenson, 2017). The core of the trade war is the semiconductor industry (Capri, 2020). The US government has reached an agreement with TSMC to build 5nm chip foundry in Arizona that costs $12 billion. NDAA Year 2021 contains initiatives to strengthen US capabilities. Discussions about potential additional restrictions on American technology, techniques, and intellectual property that help China's progress continue (M. Mutter, 2021).

Trade tensions between the US and China are only one manifestation of a growing systemic

conflict between the world's great powers. This rivalry spanned the entire geopolitical spectrum, containing both hard and soft power, with fundamental ideological differences between the two regimes beginning to impact problems other than US-China trade. Regarding structural differences between the US and China, one could argue that the interconnected network of the international supply chain has resulted in a sort of de facto strategic alliance over the last 30 years. Following decades of globalization in which offshore production became the rule, the trade environment has moved towards a more fragmented and limited in scope trade model, which some of to as "techno-nationalism." "Techno-nationalism" refers to a collection of mercantilist policies that relate technological innovation and business with a country's defence strategies, economic growth, and social stability. In this context, government interventions in markets are viewed as a form of defence against what it perceives to be opportunistic or hostile foreign actors (both state and non-state) and also as imply of developing, enhancing, and promoting its own national interest prospects (Capri, 2020).

The Trump administration accuses China of currency manipulation after the Chinese central bank allows the yuan to fall significantly. The label is highly symbolic, but it comes less than a week after Trump announced higher tariffs on $300 billion in goods. This means that everything imported into the United States from China will now be taxed. Beijing warns that the regulation will "trigger financial market turmoil (CFR.org Editor, 2022).

The Better Utilization of Investments Leading to Development Act of 2018 (P.L. 115-254) was passed by the US Congress in 2018 to provide alternatives to Chinese global projects. In addition, in collaboration with Japan and Australia, the Trump Administration established the Infrastructure Technology Assistance Network, the Transaction Advisory Fund, and the Blue Dot Network. An Executive Order (E.O.) issued in May 2020 calls for the removal of Chinese and Russian equipment from the US power grid (M. Mutter, 2021). In 2018, John McCain introduced legislation (P.L. 115-232) in Congress to strengthen US authorities. (McCain & Reed, 2019).

However, some members of Congress are concerned that the US Department of Commerce's Bureau of Industry and Security (BIS) has been hesitant to create regulations on basic and innovative products, and that gaps in US authority over greenfield and venture capital investments remain. The Trump Administration barred China Mobile and China Telecom from entering the American market, in addition to establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector and tightening licensing requirements for dual-use exports (M. Mutter, 2021).

US-China Cybersecurity Relations Under the Trump Administration

Many people have called Donald Trump a "game changer." However, there is debate over whether he significantly affected US foreign policy in ways that can be sustained. Some believe that Trump's presidency has triggered the United States' decline as a global power and/or killed liberal internationalism. Others argue that President Trump's foreign policy was defined by consistency rather than change, based on his rhetoric and performance (Ashbee & Hurst, 2021).

In the first place, President Trump is preoccupied with topics such as the trade imbalance. Furthermore, it is evident that he may take advantage of the opportunity to produce short-term, superficial outcomes. Of course, it is also conceivable that he may agree to ineffective discussions and a lack of outcomes, similar to the February 2019 meeting with North Korea in Vietnam. The important thing to remember is that, in a slightly different vein from President Trump's actions, the entire government is rapidly and significantly changing its China policy, with Congress working closely together across party lines. How far this movement will spread is still impossible to predict. Regarding its goals, the administration has not given any justification. These are the China policy weaknesses of the current Trump administration (Kubo, 2019).

One of the more ambitious actions describes US cybersecurity strategy was the Trump administration's "defending forward" concept. Defending forward was part of a larger strategic plan. Cyber capability development was not a top priority. Instead, officials attempted to restructure US national security policy so

that it would be more focused on traditional state and geopolitical threats. Threats and responses were determined by the level of national strategy. Priorities in cybersecurity came next. Defending forward, like previous cybersecurity agendas, included a call for international cooperation and norm-building, but no larger framework or context in which these should be developed. In practice, defending forward appears to be less dramatic than advertised (Shively, 2021).

Claims that the Trump administration "transformed" US policy towards China cannot be assumed quickly. Although there is a change in policy direction, the next administration will not necessarily follow Trump's policy towards China (Ashbee & Hurst, 2021) The occurrence of the trade war to the global crisis and the possibility of innovation that could lead to the escape from the crisis, the US-China trade war contributes to understanding. Without a doubt, the trade war between the U.S and China is a result of the globalization problem and its restructuring (Vlados, 2020).

Under Section 301 of the Trade Act of 1974, the United States Trade Representative (USTR) reported in 2018 that China engages in forced technology transfer, cyber-enabled theft of American intellectual property and trade secrets, discriminatory and nonmarket licensing practices, and state-funded strategic acquisitions of American assets (Andres B. Schwarzenberg, 2022). As a result, the United States imposed tariffs totaling approximately $250 billion on Chinese imports (Blumberg, 2018). China's response was to impose tariffs on $110 billion worth of American goods (Mullen & Lobosco, 2018).

U.S and China agreed to a phase-one agreement in January 2020, but most of the U.S. issues remained unsettled. Ratify the agreement to improve IP enforcement and expand access to banking and agricultural services. As part of the agreement, China agreed to purchase American goods and services for $468 billion over the course of two years. China's purchases in the first year in 2020 were significantly below 2017 trade levels in many sectors and below its obligations. In order to counter China's overcapacity, the US government also slapped tariffs on aluminum and steel in 2018 (Promuk, 2020).

In order to stop China's economic espionage, the Trump Administration has enhanced law

enforcement operations, enhanced examination of academic links to China, enforced standing rules requiring institutions and researchers to declare foreign financing, and shut down the Chinese consulate in Houston (Wong et al., 2020).

There is a plan to ban WeChat and TikTok in China (Financial Time, 2020). In November 2019, the intergovernmental Committee on Foreign Investment in the United States (CFIUS) launched a national security investigation into ByteDance. These reports came in response to direct requests from members of Congress to CFIUS to investigate TikTok's acquisition of Musical.ly (Harwell & Romm, 2019).

U.s. sen. Marco Rubio claims that there is "sufficient and growing evidence" that TikTok is removing content that goes against "orders by the Chinese government and Communist Party," including information about Hong Kong protests. U.s. senator Chuck Schumer and Tom Cotton criticized the potential national security risks posed by TikTok users' collection of personal information and the app's content censorship practices in a separate letter to Acting Director of National Intelligence Joseph Maguire. The difficulty of "data security as national security" is demonstrated by US claims against TikTok regarding data practices. Although Trump's executive order targeting ByteDance on August 6, 2020 was unusual, CFIUS has previously expressed concern about Chinese companies gaining access to U.S. citizen data (Williams, 2019).

CFIUS blocked Chinese financial technology giant Ant Group's planned $1.2 billion acquisition of US funds transfer company MoneyGram International Inc, in January 2018 (Wu & Wang, 2020). The Trump Administration authorized a ban on high-risk information and communication technology (ICT) transactions through an Executive Order. Concerned about sanctions violations, intellectual property theft, and espionage, the United States restricted technology exports to by adding Huawei and its partners to the BIS Entity List, which needs a license for the sale or transfer of US technology but did allow special cases. The BIS changed the rules to make it more difficult for Huawei to buy semiconductor chips from foreign companies that use American technology, such as Taiwan Semiconductor Manufacturing Company (TSMC)

(M. Mutter, 2021). The US government restricted the use of public funds to purchase Huawei equipment and urged foreign countries not to implement Huawei 5G network technology (Higgins, 2019).

The Trump Administration labelled China's actions in Xinjiang as human rights violations and genocide, added 54 companies to the BIS Entity List, sanctioned particular authorities and companies, issued a statement banning imports from China connected to labor exploitation, and released an advisory warning firm with Xinjiang trade exposure. China declared unconstitutional Hong Kong's special trade treatment and declared illegal certain officials after passing a national security law (M. Mutter, 2021).

The Holding Foreign Companies Accountable Act (P.L. 116-222) presupposes reporting on Chinese firms' state connections as well as the blacklisting of companies that fail to meet US conditioned on the occurrence. An Executive Order authorised in November 2020 prevents US investment in Chinese military-related companies and requires these companies to be removed from the list from US exchanges (M. Mutter, 2021).

CONCLUSION

This article has explained the changes in the US cybersecurity policy toward China under the Trump administration, precisely when the US government started to adopt a protectionist approach in 2019 following the massive expansion of China's technological and internet products into the US market. The US, in this case, ban the operation of China's software and hardware in the US. Furthermore, this research explored how such changes affected the larger trade war between the two countries, which President Trump previously started.

The impact of cybersecurity on the China-US trade war is in terms of the competition for customer data, which is the source of big data for each of the two countries' big technology businesses. For the advantage of each nation, indicating that cybersecurity is not the main reason, but economic reasons are the main reasons countries in terms of trade conflicts in the economic sector. As described, the Trump administration provided a good environment for the growth of the national technology business in the US by banning foreign products so that the US businesses could improve with the technological advancements described in the result of this

research. The Trump administration has also made policies related to the digital economy closely related to cyber. This protectionist decision has been started since the Obama administration. Trump's policies were also consistent with the previous decision made by Obama in 2015 with Chinese semiconductor and artificial intelligence technology. By giving funds for the development of the United States Cybersecurity Office, Trump has demonstrated his policies on building a good cybersecurity environment.

BIBLIOGRAPHY

Book

Ghernaouti, S. (2013). Cyber Power: Crime, Conflict and Security in Cyberspace. In *Cyber Power: Crime, Conflict and Security in Cyberspace*. EPFL Press.

Liang, G., & Ding, H. (2020). The China-US Trade War. In *Routledge Focus on Economic and Finance*. Routledge. https://doi.org/10.4324/9780429345241

Valeriano, B., & Maness, R. C. (2018). International Relations Theory and Cyber Security. In C. Brown & R. Eckersley (Eds.), *The Oxford Handbook of International Political Theory* (Issue June, pp. 258–272). Oxford University Press. ttps://doi.org/10.1093/oxfordhb/9780198746928.013.19

Journal

Al-Fadhat, F. & Prasetio, H. (2022). How China's Debt-Trap Diplomacy Works in African Countries: Evidence from Zimbabwe, Cameroon, and Djibouti. *Journal of Asian and African Studies*, 1-21. https://doi.org/10.1177/00219096221137

Arežina, S. (2019). U.S.-China Relations Under the Trump Administration: Changes and Challenges. *China Quarterly of International Strategic Studies*, *05*(03), 289–315. https://doi.org/10.1142/S2377740019500210

Ashbee, E., & Hurst, S. (2021). The Trump administration and China: policy continuity or transformation? *Policy Studies*, *42*(5–6), 720–737. https://doi.org/10.1080/01442872.2021.1919299

Barrinha, A., & Renard, T. (2017). Cyber - diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Beitelman, D.A. (2020). Living with Giants and Inconvenient

Truths: The US, China, and Everyone Else. *American Review of Canadian Studies*, *50*(1), 86-102. https://doi.org/10.1080/02722011.2020.1743001

Chong, T. T. L., & Li, X. (2019). Understanding the China–US trade war: causes, economic impact, and the worst-case scenario. *Economic and Political Studies*, *7*(2), 185–202. https://doi.org/10.1080/20954816.2019.1595328

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica*, *10*(2), 113–128. https://doi.org/https://doi.org/10.22212/jp.v10i1.1447

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review*, *27*(3), 221–244. https://doi.org/10.1177/0192512106064462

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. http://www.jstor.org/stable/27735139

Kubo, F. (2019). Reading the Trump Administration's China Policy. *Asia-Pacific Review*, *26*(1), 58–76. https://doi.org/10.1080/13439006.2019.1633153

Kusnanto, A. (2003). KEAMANAN NASIONAL, PERTAHANAN NEGARA, DAN KETERTIBAN UMUM. *Seminar Pembangunan Hukum Nasional VllI Diselenggarakan Oleh Badan Pembinaan Hukum Nasional, Departemen Kehakiman Dan HAM RI*, 1–10.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse*, *8*(1), 100–115. https://doi.org/10.1080/23269995.2017.1415082

Liu, T., & Woo, W. T. (2018). Understanding the U.S.-China Trade War. *China Economic Journal*, *11*(3), 319–340. https://doi.org/10.1080/17538963.2018.1516256

Mendhurwar, S. & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. *Enterprise Information Systems*, *15*(4), 565-584. https://doi.org/10.1080/17517575.2019.1600041

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. *Journal of Cyber Policy*, *1*(1), 5–28. https://doi.org/10.1080/23738871.2016.1157619

Nye, Jr., J. S. (2011). Nuclear Lessons for Cyber Security ? *Strategic Studies Quarterly*, *5*(4), 18–38. https://www.jstor.org/stable/10.2307/26270536

Qiu, L. D., Zhan, C., & Wei, X. (2019). An analysis of the China–US trade war through the lens of the trade literature. *Economic and Political Studies*, *7*(2), 148–168. https://doi.org/10.1080/20954816.2019.1595329

Sahide, A. (2021). Proteksionisme Trump dan Masa Depan Supremasi Politik AS. *Jurnal Ilmiah Hubungan Internasional*, *17*(1), 1-16. https://doi.org/10.26593/jihi.v17i1.3570.1-16

Segal, A. M. (2014). Cyberspace: The New Strategic Realm in US–China Relations. *Strategic Analysis*, *38*(4), 577–581. https://doi.org/10.1080/09700161.2014.918447

Shively, J. (2021). Cybersecurity policy and the Trump administration. *Policy Studies*, *42*(5–6), 738–754. https://doi.org/10.1080/01442872.2021.1947482

Sun, H. (2019). US-China Tech War: Impacts and Prospects. *China Quarterly of International Strategic Studies*. https://doi.org/10.1142/S237774001950012X

Vlados, C. (2020). The Dynamics of the Current Global Restructuring and Contemporary Framework of the US–China Trade War. *Global Journal of Emerging Market Economies*, *12*(1), 4–23. https://doi.org/10.1177/0974910119896636

Zwitter, A. (2015). Big Data and International Relations. *Ethics & International Affairs*, *29*(4), 377–389. https://doi.org/10.1017/S0892679415000362

Websites

Blumberg, Y. (2018). *Trump's $250 billion in China tariffs are now in effect—here's what could get more expensive*. CNBC. the US government imposes duties on imports from China totaling about $250 billion

Financial Time. (2020). *Why TikTok and WeChat are the new front line in the US-China tech war | FT*. Financial Time Youtube

Channel. https://www.youtube.com/watch?v=499RsH8HgJo

Harwell, D., & Romm, T. (2019). *U.S. government investigating TikTok over national security concerns*. Washingtonpost.Com. https://www.washingtonpost.com/technology/2019/11/01/us-government-investigating-tiktok-over-national-security-concerns/

Higgins, T. (2019). *Trump declares national emergency over threats against US technology amid campaign against Huawei*. CNBC. https://www.cnbc.com/2019/05/15/trump-signs-executive-order-declaring-national-emergency-over-threats-against-us-technology.html

Mullen, J., & Lobosco, K. (2018). *Trump's trade war with China just got a whole lot bigger*. CNN. https://edition.cnn.com/2018/09/23/politics/trump-trade-war-china/index.html

Promuk, J. (2020). *Trump signs 'phase one' trade deal with China in push to stop economic conflict*. CNBC. https://www.cnbc.com/2020/01/15/trump-and-china-sign-phase-one-trade-agreement.html

Sukri, A. (2020). *From trade to TikTok: How US-China decoupling affects everyone*. Www.Aljazeera.Com. https://www.aljazeera.com/economy/2020/8/4/from-trade-to-tiktok-how-us-china-decoupling-affects-everyone

Trend J., B., Balassa, B., Allais, M., Robinson, R., & Wonnacot, P. (2020). *international trade*. Encyclopedia Britannica. https://www.britannica.com/topic/international-trade

University System of Georgia. (2022). *A Brief History of the Internet*. University System of Georgia. https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml

Williams, R. D. (2019). *Reflections on TikTok and Data Privacy as National Security*. Lawfareblog.Com. https://www.lawfareblog.com/reflections-tiktok-and-data-privacy-national-security

Wong, E., Jakes, L., & Myers, S. L. (2020). *U.S. Orders China to Close Houston Consulate, Citing Efforts to Steal Trade Secrets*. New York Times. https://www.nytimes.com/2020/07/22/world/asia/us-china-houston-consulate.html

Wu, K., & Wang, E. (2020). *FACTBOX-U.S. government panel cracks down on Chinese deals*. Reuters.Com. https://www.reuters.com/article/usa-election-china-investments-idUSL4N2HC14X

Report

Capri, A. (2020). *Semiconductors at the Heart of the US-China Tech War; How a New Era of Techno-Nationalism is Shaking up Semiconductor Value Chains*.

Dupont, A. (2020). *Mitigating the New Cold War: Managing US-China trade, tech and geopolitical conflict* (Issue May).

Williams, R. D. (2020). *Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security*. https://www.brookings.edu/research/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/

Ikenson, D. (2017). Cybersecurity or Protectionism: Defusing the Most Volatile Issue in the U.S.-China Relationship. In *Cato Institute* (Issue 815). https://www.cato.org/policy-analysis/cybersecurity-or-protectionism-defusing-most-volatile-issue-us-china-relationship#:~:text=Defusing the Most Volatile Issue in the U.S.–China Relationship,-July 13%2C 2017&text=For several years%2C Chinese information,t

Government Publication

Andres B. Schwarzenberg. (2022). Section 301 of the Trade Act of 1974. In *Crs*. https://crsreports.congress.gov/product/pdf/IF/IF11346

M. Mutter, K. (2021). *U.S.-China Trade Relations* (Issue February 2021). https://crsreports.congress.gov/product/pdf/IF/IF11284

McCain, J., & Reed, J. (2019). *National Defence Authorization Act for Fiscal Year 2019*. https://www.armed-services.senate.gov/imo/media/doc/FY19 NDAA Executive Summary FINAL.pdf

The White House. (2020). *Executive Order on Addressing the Threat Posed by TikTok*. Whitehouse.Org. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/