View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Jurnal Ilmiah Hubungan Internasional

https://doi.org/10.26593/jihi.v16i2.4204.159-178

The Securitization of Chinese Technology Companies in the United States of America

Giandi Kartasasmita[1] and Andrea Prisca Kurnadi[2]

[1] Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Katolik Parahyangan, Indonesia, giandi@unpar.ac.id
[2] Faculty of Business and Social Sciences, International University Liaison Indonesia, Indonesia, andrea.kurnadi@iuli.ac.id

ABSTRACT

This paper aims to explain the securitization process of Chinese technology companies by the U.S Government. While the U.S has been aware of the cyber threat since 1998, before Trump's presidency, the U.S. Government had never taken drastic measures against foreign technology companies based on national security pretext. This paper revealed that the U.S. Executive has succeeded in securitizing the Chinese hardware and software companies, perceiving Chinese companies as an existential threat to U.S security, privacy, and liberty. This move leads to the increasing number of U.S. Citizens perceiving China as a significant threat to the U.S.

Keywords: *Securitization, cyber threat, technology, cyber security, technology companies*

ABSTRAK

Tulisan ini menjelaskan proses sekuritisasi perusahaan teknologi Tiongkok oleh pemerintah Amerika Serikat. Meskipun Amerika Serikat dari tahun 1998 telah memiliki kesadaran akan bahaya siber, sebelum pemerintahan Presiden Donald J. Trump di tahun 2016, pemerintah Amerika Serikat tidak pernah melakukan tindakan yang drastis terhadap perusahaan teknologi dari negara lain berdasarkan alasan keamanan nasional. Tulisan ini menemukan bahwa Pemerintahan Presiden Trump sukses melakukan sekuritisasi terhadap keberadaan perusahaan teknologi perangkat keras dan perangkat lunak Tiongkok, membangun persepsi ancaman terhadap keamanan, privasi dan kebebasan di Amerika Serikat. Langkah yang diambil meningkatkan persepsi ancaman warga negara Amerika Serikat terhadap Tiongkok.

Kata kunci: Sekuritisasi, ancaman siber, teknologi, keamanan siber, perusahaan teknologi

> "…. the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States".
>
> Executive Order, May 15, 2019
>
> Donald J. Trump, President of The United States of America

This writing is about U.S-China cyber interaction and the shifting notion of threat in Cyberspace. We argue that the U.S. ban on Chinese telecommunication companies is based on the growing insecurity of President Trump Administration against increasing adversaries'

parity in Cyberspace. The issue is securitized in the sense that China's telecommunication companies are considered as China's Communist Party cyber tools and hence became an imminent threat to the U.S.

The U.S. and China-owned Technology Companies Fray

In 2018, Trump Administration enacted a 7-year sales ban, which prohibits American companies from doing business with the Chinese company ZTE Corporation due to ZTE's involvement in U.S. technology's unauthorized sales to Iran and North Korea.[1] ZTE pleaded guilty, paid a 1 billion dollars penalty, and allowed the U.S. special committee to oversee ZTE compliance with U.S. regulation and rules. Thus the U.S. Government temporarily lifted the ban, which will enable ZTE to resume business with American Companies[2]. However, on May 15, 2019, President Trump signed an Executive Order, which gives the Secretary of Commerce the power to determine potential national security risk in U.S. foreign trade and block highly national security risks transactions[3]. As a result, ZTE is perceived as a National Security risk and banned from conducting any business in the U.S.

The executive order also targeted Huawei, a China-based telecommunication hardware giant. Huawei has built a massive network of 4G infrastructures in 170 countries and 5G infrastructure in 54 countries, making Huawei the largest communication provider globally.[4] The Trump administration perceives Huawei's market dominance as a threat to U.S. National Security. The U.S. accused Huawei of under China's military's influence[5] and accused Huawei of installing a covert "back door" in its network infrastructures, which allows the People's Republic of China to exploit it for their cyber-espionage agenda[6]. Thus, President Trump banned U.S. Companies from using Huawei made equipment and prohibiting Huawei from using the U.S. made supplies and technologies. President Trump's ban on ZTE and Huawei has gained bipartisan support from both GOP and Democrat in Congress. Democrat Senator Mark Warner and Republican Senator Marco Rubio introduced a bipartisan bill to address China's technology company's threat to the U.S.[7] The

[1] Robert Delaney. 2018. *US slaps China's ZTE with 7-year components ban for breaching terms of sanctions settlement.* South China Morning Post 16 April 2018. Retrieved 27 August 2020. https://www.scmp.com/business/companies/article/2142002/us-slaps-zte-seven-year-components-ban-breaching-terms-sanctions

[2] Brenda Stolyar and Christian de Looper. 2018. *ZTE and the U.S.: Everything you need to know.* Digital Trends 13 April 2018. Retrieved 27 August 2020. https://www.digitaltrends.com/mobile/commerce-bans-zte-from-exporting-technology-from-the-us/

[3] The White House. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. 15 May 2019. Retrieved 26 August 2020. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[4] Emily Feng, and Amy Cheng. 2019. *China's Tech Giant Huawei Spans Much Of The Globe Despite U.S. Efforts To Ban It.* National Public Radio (npr.org) 24 October 2019. Retrieved 27 August 2020. https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it

[5] Corrinne Reichert. 2020. *Huawei is backed by Chinese military, Trump administration finds.* 2020. CNET 24 June 2020. Retrieved 27 August 2020. https://www.cnet.com/news/huawei-is-backed-by-chinese-military-trump-administration-reportedly-finds/

[6] Corinne Reichert. 2020. *US finds Huawei has backdoor access to mobile networks globally, report says.*CNET 12 February 2020. Retrieved 27 August 2020. https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/

[7] Alfred Ng. 2019. *Senators introduce bipartisan bill to address Chinese tech concerns.* CNET 4 January

policy not only weakens the Huawei telecommunication business sector but significantly affects Huawei's dominant position in the smartphone market because Huawei relies on Google, Arm, and Qualcomm, three US-based technology giants in mobile devices. To make things worse, On May 13, 2019, the Trump administration extend the executive bill until May 23, 2021.[8]

Many U.S. technology companies oppose such a ban. Brad Smith, Microsoft chief legal officer, claims that the Trump administration has not provided enough evidence of national security threat as justification for the ongoing ban on Huawei.[9] Google calls the Huawei ban as a national security risk due to the possibility that the ban will force millions of devices to migrate to Huawei's operating system Hongmeng, which will be susceptible to get hacked by the Chinese Government.[10] Rural communication carriers are also opposing such a ban. These communication companies tend to rely on cost-effective Huawei devices. Replacing all Huawei devices with other brands will raise the operational costs and will harm the rural telecommunication business and its consumers.[11] Similar concerns also came from US-based Huawei suppliers. In 2018, Huawei spent 11 billion dollars on supply from U.S. companies in Idaho, Wisconsin, Kentucky, Michigan, Arizona, California, and New York; the ban will significantly lower companies' income[12] and harm domestic jobs.[13]

The U.S. Attack on Huawei had started before the Executive order. In December 2018, at the U.S. request, Canada arrested Huawei CFO Meng Wanzhou on the accusation that Huawei was involved in illegal sales of U.S. technology to Iran[14]; later Canadian Court in Vancouver, British Columbia, ruled that Wangzhou is eligible for the extradition process to the U.S.[15], further damaging US-China

---

2019. Retrieved 27 August 2020. https://www.cnet.com/news/senators-introduce-bipartisan-bill-to-address-chinese-tech-concerns/

[8] Brian Heater 2020. *Trump adds another year to Huawei/ZTE ban.* TechCrunch 15 May 2020. Retrieved 27 August 2020. https://techcrunch.com/2020/05/14/trump-adds-another-year-to-huawei-zte-ban/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGhucOEibiuOrvFD8hkQP-q1yzfMhR8gyE1gAEB__BwhN0UALH7roB9mmbR8tMdpK0_gSLf8LZPijexF2o-vJsXgwFG2m3r_-zDa-J0GKtjE2EueF5IKMHyfGOr8u3ZM8L4ncglz9RAXQb6ir4Ee0I_lBr9sWhAMTwL9Xnuq8fvg&guccounter=2

[9] Dina Bass. 2019. *Microsoft Says Trump Is Treating Huawei Unfairly*. Bloomberg 8 September 2019. Retrieved 27 August 2020. https://www.bloomberg.com/news/articles/2019-09-08/microsoft-says-trump-is-treating-huawei-unfairly

[10] Financial Times. 2019. *Google warns of US national security risks from Huawei ban.* Financial Times. Retrieved 27 August 2020. https://www.ft.com/content/3bbb6fec-88c5-11e9-a028-86cea8523dc2

[11] Zen Soo. 2019. *Trump's Huawei ban will hit rural US carriers the hardest as replacing equipment will cost 'millions'*. South China Morning Post 4 March 2019. Retrieved 27 August 2020. https://www.scmp.com/tech/enterprises/article/2188422/trumps-huawei-ban-will-hit-rural-us-carriers-hardest-replacing

[12] Corrine Reichert and Marguerite Reardon. 2019. *Huawei says US ban will 'significantly harm' American jobs, companies.* CNET 16 May 2019. Retrieved 27 August 2020. https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-american-companies-jobs/

[13] Sean Keane. 2019. *Huawei lays off hundreds of US workers due to blacklisting.* CNET 23 July 2019. Retrieved 17 August 2020. https://www.cnet.com/news/huawei-lays-off-hundreds-of-us-workers-due-to-blacklisting/

[14] Steven Musli. 2018. *Huawei executive arrested in Canada at US request.* CNET 6 December 2018. Retrieved 26 August 2020. https://www.cnet.com/news/huawei-executive-arrested-by-canadian-officials-at-us-request/

[15] Tracy Sherlock and Dan Bilefsky. 2020. *Extradition of Huawei Executive Clears a Major Legal Hurdle in Canada.* The New York Times 27 May 2020. Retrieved 27 August 2020. https://www.nytimes.com/2020/05/27/world/canada/huawei-extradition-meng-wanzhou.html

relations. The U.S. also persuaded allies to ban Huawei's involvement in developing 5G infrastructure in their countries.[16] Japan, Australia, New Zealand, Canada[17], the U.K.[18] , and India[19] follow the U.S. in banning Huawei in developing 5G infrastructures, while European Union Countries allow some Huawei equipment in their non-core 5G networks.[20]

Federal Communications Commission (FCC) also put pressure on China by starting the process of revoking business licenses for 3 Chinese telecom companies; China Telecom, China Unicom, and ComNet that has been operating in the U.S. for more than a decade[21]. FCC also denied China Telecom application to provide telecommunication services in the U.S. because of security concerns that it can be used by the Chinese Communist Party to conduct espionage against the U.S."

In the latest volley of attack against China telecommunication companies, on August 5, 2020, Secretary of State Mike Pompeo announced the Clean Network Program, which takes an anti-Chinese position to eliminate Chinese technology out of U.S.' internet and network. The Clean Network program will revoke all Chinese telecommunication carriers, cloud services, undersea cables, applications, and application stores.[22] The program is expanding the White House's 5G Clean Path initiative to prohibit Chinese hardware companies, such as Huawei and ZTE, out of U.S.' telecommunication infrastructure.

Using this initiative, on August 6, 2020, U.S. Government escalated its aggression against China by issuing two executive orders[23] on addressing the threat posed by Tiktok and WeChat. Trump accuses Tiktok and WeChat of political censoring and potential misinformation campaign.[24] Bytedance, the owner of Tiktok, and Tencent, the owner of the massaging platform WeChat is given 45 days to sell their respective apps to U.S. companies or faced a ban on the

---

[16] Robin Emmott. 2018. *U.S. warns European allies not to use Chinese gear for 5G networks.* Reuters 5 February 2018. Retrieved 26 August 2020. https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG

[17] Emily Feng, and Amy Cheng. 2019. *China's Tech Giant Huawei Spans Much Of The Globe Despite U.S. Efforts To Ban It.* National Public Radio (npr.org) 24 October 2019. Retrieved 27 August 2020. https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it

[18] Katie Collins. 2020. *UK follows US in banning Huawei from 5G network*. CNET 14 July 2020. Retrieved 27 August 2020. https://www.cnet.com/news/uk-follows-us-in-banning-huawei-from-5g-network/

[19] Archana Chaudhary, Ragini Saxena, PR Sanjai, and Saritha Rai. 2020. *China's Huawei, ZTE Set To Be Shut Out of India's 5G Trials.* Bloomberg 14 August 2020. Retrieved 27 August 2020. https://www.bloomberg.com/news/articles/2020-08-13/china-s-huawei-zte-set-to-be-shut-out-of-india-s-5g-trials?cmpid=socialflow-twitter-business&utm_source=twitter&utm_campaign=socialflow-organic&utm_content=business&utm_medium=social

[20] European Commission. *Secure 5G networks: Commission endorses EU toolbox and sets out next steps.* 29 January 2020. Retrieved 25 August 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

[21] Venturebeat. 2020. *FCC finalizes Huawei and ZTE ban, citing threats to U.S. security*. Venturebeat.com 30 June 2020. Retrieved 27 August 2020. https://venturebeat.com/2020/06/30/fcc-finalizes-huawei-and-zte-ban-citing-threats-to-u-s-security/

[22] U.S. Department of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets,* August 5, 2020, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

[23] White House, *Executive orders on addressing the Threat Posed by Tiktok,* August 6, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/ and White House, *Executive orders on addressing the Threat Posed by WeChat,* August 6, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/

[24] *Ibid.*

U.S. Tiktok later sues the Trump administration[25] , and a petition is raised calling the Government not to ban WeChat[26].

The latest executive order sends domestic shockwaves. Tiktok is very popular among the U.S. teens, and WeChat is the only available messaging apps in China; thus, banning WeChat is also blocking the ability of the Chinese community in the U.S. to communicate with relatives in China and also hinder the ability of U.S. Business to communicate with its business counterpart in China. It also can be perceived as an unwelcome signal to the Chinese community in the U.S. [27]

The Chinese Government has vowed to retaliate against unfair treatment to its technology and telecommunication companies. China says, "China will take forceful countermeasures to protect its legitimate rights."[28] and has planning to put major U.S. technology companies such as Apple, Cisco, and Qualcomm in unreliable entity list and restricting these companies to conduct business in China.

While the U.S. government has taken Cyberspace as national security consideration since President Bill Clinton signed Presidential Decision Directive 63 in 1998, U.S. Government had never authorized such a dramatic move against foreign companies from China under the pretext of national security before Trump's Presidency.

Understanding the Threat in Cyberspace

What constitutes Cyberspace of the internet has evolved from a realm of communication and e-commerce to "critical infrastructures." The critical infrastructures are the underlying sectors that run modern-day civilization, ranging from agriculture, food distribution, banking, healthcare, transportation, water, and the power grid.[29] Each of these once stood apart but now are all bound together and linked into Cyberspace via I.T.

The reliance on private sectors in Cyberspace is relatively high. The private sectors provide cyberinfrastructure, use Cyberspace to control critical infrastructure on the flow of water, deliver electricity to our home, and execute the financial transactions that keep currency prices stable. Cyberspace, thus, evolving from only "a nervous system"[30] into something more advanced. Cyberspace is now becoming "the dominant platform for life in the 21st century".[31]

Since the 1990s, the U.S. government under Bill Clinton administration has predicted that the internet would be part of national security concern. The distinguishing feature of the internet is that protection against adversaries in Cyberspace is more complicated than traditional spaces—air, land, water, and space. First, Cyberspace has no actual border where any government could claim dan regulate.[32] Second,

---

[25] Mike Isaac and Ana Swanson. 2020. *TikTok Sues U.S. Government Over Trump Ban.* The New York Times 24 August 2020. Retrieved 27 August 2020. https://www.nytimes.com/2020/08/24/technology/tiktok-sues-us-government-over-trump-ban.html

[26] Petitions. *WeChat Should Not Be Banned.* The White House 14 July 2020. https://petitions.whitehouse.gov/petition/wechat-should-not-be-banned

[27] Feng Zhaoyin and Joshua Cheetam. 2020. *Trump WeChat ban 'an unwelcome signal' for Chinese community.* BBC News 10 August 2020. https://www.bbc.com/news/world-asia-china-53686507

[28] Venturebeat. 2020. *China asks U.S. to stop 'unreasonable suppression' of Huawei.* Venturebeat.com 16 May 2020. Retrieved 27 August 2020. https://venturebeat.com/2020/05/16/china-asks-u-s-to-stop-unreasonable-suppression-of-huawei/

[29] P,W. Singer and Allan Friedman, 2014, *Cybersecurity and Cyberwar: What Everyone Needs to Know,* NY: Oxford University Press, p.15

[30] The control system of our economy.

[31] P.W. Singer and Alan Friedman, *Op.Cit.,* p.16

[32] Derek S. Reveron, 2012, *Cyberspace and National Security: Threats, Opportunities, and Power in a*

there are many internets—not only one, hence shutting down the internet is nearly impossible. Third, multiple actors (individuals, businesses, and Government) exist and interact in the Cyberspace. Forth, our daily life is connected to the internet, ranging from banking, e-commerce, gaming to news portals and social media.

The January 2010 Stuxnet worm hijacked the Iranian Nuclear plant was the turning point for the U.S. Following the Stuxnet incident, and the U.S. Defense Department highlighted that Cyberspace is now considered the domain for defense activities, as natural as the traditional spaces.[33] Nevertheless, way long before Stuxnet, Cyberspace had already taken into national security consideration when in 1998, President Bill Clinton signed Presidential Decision Directive 63, which established a White House structure to coordinate Government and private action to "eliminate any significant vulnerability to both physical and cyberattacks on our critical infrastructures, including especially our cyber systems."[34] In 2005 and 2008, the National Defense Strategy identified Cyberspace as a new theater of military operations and explored Cyberspace as a potentially disruptive challenge. They further concluded that individuals, small groups, or foreign adversaries could attack and disrupt commerce and daily life in the U.S., causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks.[35] The 2011 National Military Strategy identified that the expansion and intensification of threats in Cyberspace are because of a lack of international norms, low barriers to entry, difficulties of attribution, and the relative ease of developing powerful—offense capabilities.[36] Moreover, in 2012, strategic defense guidance formulated one of the U.S. armed forces' primary missions to operate effectively in Cyberspace.[37]

The problem is that recognizing the cyber threat as part of national security concerns is only the beginning, acknowledging the problem did not equal taking actions in solving it. In the U.S, a clear gap existed between policy and law regarding Cyberspace. U.S Government had not figured out what role could and should the Defense Department play in the Cyberspace area. In 2008 Center for Strategic and International Studies, a well-known U.S think-tank urged the U.S Government to address the issue, stating that "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[38] Former North Atlantic Treaty Organization (NATO) commanders, Ret Army General Wesley K. Clark and Ret. Army General Peter L. Levin, also warned the U.S about the evident threat of Cyber Security. Both General concerned that the U.S. Government could no longer afford to ignore the consequences from offenses on cyber realms targeted its vital services and infrastructures.[39]

Before 2018, the U.S. disparage foreign adversaries' cyber espionage, cyber intrusion, and cyberattacks abilities to generate destruction and still profusely focusing on stopping physical attacks by terrorists or through other states' physical attacks in traditional spaces. The U.S National Security Strategy (NSS) outlines the United States' major national security concerns and how the administration plans to deal with them. Until 2006, the U.S NSS has not included cybersecurity as part of its national security

---

Virtual World, Washington D.C: Georgetown University Press, p.6

[33] *Ibid.,* p.7

[34] *Ibid.,* p.8-9

[35] *Ibid.,* p.9

[36] *Ibid*

[37] *Ibid*

[38] *Ibid*

[39] *Ibid*

concern.[40] George W. Bush Administration issued 2002 and 2006 NSS, and the foremost security concern was about global terrorism, the threat of Weapon of Mass Destruction (WMD), and defusing regional conflicts.

During Obama's presidency, a minor change took place where he defined the cyber threat as "one of the most serious economic and national security challenges we face as a nation."[41] However, in the 2010 NSS, Obama's administration as yet to ignore the existence of cyberattacks on U.S security, focusing only "to strengthen the security and resilience of U.S Critical Infrastructure."[42] A similar perspective still loomed the 2015 NSS of which the administration downsized the threat of cyberattack, mainly directed to the national network and critical infrastructures.[43] Both 2010 and 2015, NSS riveted only on the security of networks, and not on the U.S security as a whole.

A quite radical step was taken by the Trump Administration, where the 2017 NSS clearly stated that cyberattacks could harm large numbers of people and institutions; and undermine faith and confidence in democratic institutions and the global economic system.[44] The 2017 NSS explained what actions should be taken by the Government to address such attacks as well. Later in May 2018, the Department of Homeland Security issued a specific cybersecurity strategy, followed by the White House's National Cyber Strategy in September 2018.[45] Both documents emphasize protecting the American people and the U.S homeland against cyberattacks from adversaries such as China, Russia, Iran, and North Korea.[46] To achieve the goals, the Government conducts a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime.[47]

Lucas Kello argues that Cyberthreat's inadequate attention came from a common Clausewitzian mindset that looms in the U.S security apparatus and think-tanks. According to Kello, many security actors had difficulties with irregular warfare, such as cyberattacks, because the western ways of warfare until the nineteenth century did not experience this as a frequent occurrence. Clausewitz viewed the war in a world of state against state, with clear borders, to obtain a political objective. However, in Cyberspace, it is a different kind of scenario.[48] Cyberspace has no state borders, with different characteristics than traditional security[49]cyberspace poses (1) the expansion of non-physical threats to national security; (2) the dangers of unwanted or accelerating crises even among rational contenders; and (3) the growing ability of private sectors or actors to disturb standard political order. States remain the

[40] At that time the development of cyber technology was still limited, and cyber users worldwide was 361 million predominantly resided in the U.S and Europe. By 2010, major changes have in cyber technology

[41] War in the Fifth Domain, The Economist (July 1, 2010).

[42] National Security Strategy, 2010, White House, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf p.27

[43] National Security Strategy, 2015, White House, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf p.12

[44] National Security Strategy, 2017, White House, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf p.37-38

[45] Cybersecurity Strategy, U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

[46] National Cyber Security, 2018, White House, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf p.1-2

[47] *Ibid.,* p.6

[48] Greg Rattray, 2001, *Strategic Warfare in Cyberspace*, Cambridge, MA: The MIT Press, p.15

[49] Lucas Kello, *The Virtual Weapon and International Order, Op.Cit.,* p.55

principal players in the cyber domain but are no longer the only relevant actor in international relations in the cyber age. Other players can inflict significant harm in ways that propel a crisis beyond the control of governments.

In his book, Kello distinguished five difficulties in conceptualizing cyberattack by traditional measures:[50]

1. The actions lack a proximate cause of injury and may not even be violent.

2. The conception of war as the use of armed force sets a high threshold in terms of scope, duration, and intensity that cyber actions may not meet.

3. The perpetrators of a cyberattack can be a non-state who are not typically considered subjects of international law; thus, not subject to its restraining procedures.

4. An offensive cyber operation by non-traditional players, such as that conducted against Estonia by the Russian private sector, need not involve states or their military's strategic purposes.

5. At least, in the case of a generalized cyberattack, the critical distinction between military and civilian targets dissolves due to the broad diffusion of computer systems in society and their interdependencies. (Share the same WWW and cyber workspace).

Based on extrapolations of cyberattack simulation conducted by the U.S National Academy of Sciences in 2007, penetration of the U.S. electrical grid's control system could cause "hundreds or even thousands of deaths" as a result of human exposure to extreme temperature. The Clausewitzian is inadequate to address these problems. Clausewitz emphasizes that the cyber actions have no intrinsic capacity for violence, at least not on a scale of intensity and destruction that Clausewitzian prism deems relevant to theory. The reason is that the method of harm lacks similarities with interstate armed conflict. Therefore, it cannot be classified as a "threat."

Clausewitzian notions of war and peace are polar binaries; denying a major warlike is to affirm that it is peace-like.[51] Hence, there was no adequate policy from the U.S. policy-makers before 2018 about cyberwar or its potential destruction because cyberwar actions are considered not acts of war. Where others see war, skeptics find a tolerable state of comity on the emergence of an international consensus stabilized around many limited acceptable uses of cyber technology or weapons as long as it prohibits any dangerous use of force.[52]

Such a perspective misunderstands the nature of the peril. For two main reasons, a peace-like situation in Cyberspace is unsuitable.[53] First, the harmful consequences or hostile activity that falls beyond the recognized criteria of war are more significant than any previous peacetime competition in our history. The damage to national and economic security from cyberattacks and cyber espionage is conceivably more significant than some acts of war or uses of force could achieve. Nevertheless, they do not fit the definition of either war or force. In 2014, Russia attacked the NASDAQ by sending a malware code to interrupt the largest stock exchange servers.[54] If this attack succeeded, it could erode the integrity of the equity exchange that is now the heart of

[50] *Ibid.*

[51] Lucas Kello, 2017, *The Virtual Weapon and International Order,* US: Yale University Press, p.77

[52] Brandon Valeriano and Ryan Manness,2015, *Loc.Cit.,*

[53] Lucas Kello, 2017, *The Virtual Weapon and International Order, Op.Cit.* p.75

[54] Michael Riley, *How Russian Hackers Stole the NASDAQ,* Bloomberg 22 July 2014 (https://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq) Retrieved 20 October 2018

advanced economies. Because the mode or the indirect effects of this attack are not violent, the action did not consider as an act of war.

Second, the absence of war does not mean the existence of peace. In the past, statecraft's desirable objective is the situation of peace, whatever its final shape. Consequently, nation-states know that a given state of affairs violates the conceptual limit of peace when some of the system's central units no longer accept it as a desirable or even bearable state of affairs. Much of cyber activity falls between a state that neither recognized as a war nor recognized as peace. Russia and China, for example, see cyber operations as a part of warfare strategy during peacetime.[55] From this depiction, it has become difficult to distinguish a situation in which nations are at war from when they are at peace. Peace can become a form of war.

The prospect of permanent intrusion of the defender's infrastructure raised by the Cyberspace represents a reversal of the classical security paradigm. Previously, security planning's primary aim was to prevent the enemy's presence on the home terrain. In the new domain, it must be a starting assumption of strategy that the enemy is already inside. The ability of advanced adversaries to reside permanently within essential infrastructures proves a remark from British politicians Stanley Baldwin about strategic warfare in the 1930s: the bomber will always get through.[56] We now change it into a new remark "the malware will always get through.

The difficulties of detecting the foe's presence complicate the task of compellence, which Thomas Schelling described as the act of convincing an opponent to withdraw from the territory that he has invaded.[57] In cyberattack, it does not involve human agents, who, if caught, can be subjected to the full penalties of domestic legal code (and in wartime, death). No more is the nature of the threat, one merely of information seizure. Information itself has become a threat because it can disrupt the operations of or destroy vital computer infrastructures.

Thus, cyberwarfare poses a danger as much as conventional warfare. There are several reasons to defend the argument. First, there is a fundamental offense-defense imbalance, as the result of software and hardware complexity increases. Improvements in cybersecurity mechanisms (defense) lag behind the attacker's ability to launch new offensive cyber weapons (offense). The expanding network surface provides conditions for a shock offensive.[58] The former U.S. Director of CIA, George Tenet, summarized the situation by saying, "We have built our future upon a capability we have not learned to protect."[59]

Second, the total cost of a cyberattack is diminishing. What was considered a sophisticated cyberattack only a year ago might now be incorporated into a downloadable and easy to deploy Internet Application, requiring

---

[55] John Barasso, Marry Fallin and Virginia Foxx, 2016, *Republican Platform 2016,* Cleveland: Consolidated Solutions, p.53

[56] Keith Middlemas and John Barnes, 1969, *Baldwin: A Biography*, London: Weidenfeld & Nicolson, p. 72 2.

[57] Thomas Schelling, 1966, *Arms and Influence,* New Haven: Yale University Press, p. 72

[58] Our world wide web is enmeshed into a single global network and is used not only by common citizens, but also military. Shock offensive comprises the ability to choose the main point of attack for initial battle, to move forces there simultaneously and to surprise the defender.
See Lucas Kello, *Virtual Weapons and International Order, Op.Cit.,* p.73

[59] Robert O'Harrow Jr, *Understanding Cyberspace is Key to Defending Against Digital Attacks,* The Washington Post 2 June 2012 (https://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defending-againstdigital-attacks/2013/06/03/d46860f8-ad58-11e4-9c91-e9d2f9fde644_story.html?noredirect=on&utm_term=.ce434bb7eac1) Retrieved 20 October 2018

little or no expertise to use. The Stuxnet worm that attacked Natanz facility nuclear in Iran is now available for free download on the internet. Third, a cyberattack is neither required visible weapon—only a series of code, nor massive damage at first. Such an attack would be all the more damaging because, at least initially, officials would be unable to detect the source of the problem. Eventually, a particular utility of virtual weapon expands the choice of actions and outcomes available to the strategic defense for any actors: states, private sectors, terrorists, or even ordinary citizens.

The absence to date of more severe cyberattacks does not prove the impotence of the new weapon and the new type of war. It may instead indicate their severity if the fear of retaliation and blowback are restraining factors. The resistance of security studies scholars to acknowledge it and broaden the conventional perspective of war and security is correctly stated by Thomas Kuhn, "The source of resistance [to the new theory] is the assurance that the older paradigm will ultimately solve all its problem."[60]

The U.S. new administration under President Donald Trump recognizes these changes and adapt to these changes accordingly. Cyberspace and "malicious" activities on the internet are considered a real security threat to the U.S. homeland. The administration—or Trump himself, sees Cyberspace not only as a means for but also a target of intrusions from adversaries, in this sense, especially from China. However, the former U.S. President Barrack Obama has once defined the cyber threat as "one of the most serious economic and national security challenges we face as a nation," [61] no further actions taken. The U.S. officials feared that if the U.S. took such harsh action, it would set a precedent and invite other countries (China, Russia) to use similar means in the future.[62] As James Lewis, a cybersecurity expert at the Center for Strategic and International Studies, succinctly put it, "We do not want to be the ones who break the glass on this new kind of warfare."[63] Why, then, the Trump administration took such a bold action to break the glass that no one dares to?

Securitization Theory

When an issue is presented as posing an existential threat—usually to the entire nation-state, it requires emergency measures. In other words, it is "securitized."[64] This perspective of 'Securitization' first devised by Ole Wæver to provide a fresh take on the debate between two groups; those who claimed threats are objective, and those that argued that security threats are subjective. To bypass the debate, the Copenhagen School suggests that a problem becomes a threat to security not necessarily because a real existential threat exists, but because the problem is presented and established by the key agents—officials of the state. Alternatively, in other words, how a problem can be socially constructed as a threat. Securitization is based on speech act theory, where the security speech act is significant utterances in a security framework by actors with authority to define security and how to respond to the threat. An actor must do a performative act, officially state

[60] Thomas S. Kuhn, 1996, *The Structure of Scientific Revolutions* (3rd ed), Illinois: Univesity of Chicago Press, p.151

[61] War in the Fifth Domain, The Economist (July 1, 2010).

[62] Tim Maurer, *The Case of Cyberwarfare,* Foreign Policy 19 October 2011, (https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/). Retrieved 19 October 2018.

[63] Eric Schmitt and Tom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya,* The New York Times 17 October 2011, (https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1&hp) Retrieved 19 October 2018

[64] Barry Buzan, Ole Wæver and Jaap Wilde, 1998, *Security: A New Framework for Analysis*, Boulder, CO: Lynne Rienner Publishers

that a threat exists, and threatens a specific object. In short, a securitizing speech act has to fulfill three rhetorical criteria.[65] First, an actor claims that a referent object is existentially threatened. Second, it demands the right to take emergency or extraordinary measures.

Lastly, the actor convinces audiences to accept and support emergency measures—the standard outside rule or rule-breaking behavior to counter the threat is justified. Hence, by labeling an issue as security, it is exaggerated as an issue of ultimate priority. Therefore, securitization can be thought of as a process in which any issues are aggrandized to security issues requiring to be treated with exigency, legitimizing the bypassing of public debate and democratic procedures.

There are several variables or essential components to work with when studying the securitization process[66]:

1. The securitization actor securitizes an issue: mainly states representatives in a position of power who make arguments regarding the threat to the referent object. The actor can be political leaders, bureaucracies, governments (president, prime minister), and pressure groups.[67]
2. The threat subject, Copenhagen school, highlights five sectors of security, namely military, political, economic, societal, and ecological/environmental threats to national security. In each sector, a specific threat is articulated as threatening a referent object. For example, in the societal sector, the referent object is identity, while the referent objects in the economic sector are corporations.
3. The referent object: the object (in each sector) whose survival is to be both necessary and threatened. In this sense, the referent object being threatened can encompass any actor from the individual to the international level, including such actors as corporations, nations, states, and communities.
4. The intentions and purposes, why must we securitize an issue. The issues become securitized when they need extraordinary measures.[68]
5. The outcome or desired results when an issue (political or non-political) becomes a security issue.
6. The structure, under what conditions when the securitization is successful. Securitization moves are successful if an audience collectively agrees on the security argument and supports the taking of extraordinary measures.[69]

Even though Copenhagen School only distinguished five (5) sectors of security, the Buzan view of security studies accepts a much broader and deeper agenda. It is not limited only to those mentioned above, due to ever-changing and expanding issues in modern civilization. Advancement of ICT and the rise of networked devices has led to the most dramatic shifts in social interaction and social behavior over generations. In modern society, the essential infrastructure, from nuclear plants to civilian transportation networks to government computer systems, relies on functioning computers and networks. A small breakdown can disrupt and destruct the whole system. In this sense, cyberattacks and cyber warfare would constitute security issues for a referent object, even if the actor is an individual, and the existential threat is a threat of economic ruin.

[65] Barry Buzan, Ole Wæver and Jaap Wilde, *Op.Cit.,* p.23-24
[66] *Ibid.* p.32
[67] *Ibid.,* p.36, 40
[68] *Ibid.,* p.24
[69] *Ibid.,* p.25

Securitization of China's Technology Companies in the USA

Cybersecurity is a critical issue in states' national policy due to the overreliance on the internet in every aspect of life. The main concern has been the network infrastructure that contains information critical to national security, to protect it from being hacked. The protection aims to eliminate[70]: (1) threats to the confidentiality of data, such as classified data theft; (2) threats to the integrity of data, like the manipulation of financial records; and (3) threats to the availability of data, such as cyberattacks to critical infrastructures.

The Trump administration's waging technological war against China is mainly due to the differences between China and the United States in political values and geopolitical pursuits and their rivalry on regional and global arenas.[71] The U.S. attitude towards China has been tense since the steady rise of China's technological advancement in 2008.[72] President Obama administration has been attempting to prevent Chinese enterprises investing in the American semiconductor industry and gradually tightened Chinese access to American technology. However, under the Trump administration, technology competition's securitization between the U.S. and China is formally engaged.

In 2017, the world witnessed a tense relation between China and the U.S. Trade frictions and technological competition between two big powers ensue. Trump administration has regarded China as its primary competitor, and it aims to prevent the development of the Chinese's high technology industry.

China is labeled as being unethical, and its industrial planning is a government-led that enforcing technology transfer. Other allegations are China has been utilizing technology to support its authoritarian regime and that Chinese's advancement in science and technology would harm the U.S. national interests and regional order.[73] Trump administration also accused Huawei of a government-backed company. By exaggerating the issues and security risk, the U.S government has been trying to securitize the technological war against China.

The notion of government background of Chinese enterprises, especially Huawei, is based on the nature of China's s civil-military integration in the context of operations in the cyber domain. According to Tai Ming Cheung, director of the University of California Institute on Global Conflict and Cooperation, Chinese civil-military integration encompasses a diverse range of activities based on the notion of harnessing the civilian economy's technological and industrial to advance defense capabilities.[74] The defense economy seeks to make use of commercially available technologies and manufacturing processes as a suitable substitute.[75] The integration is the potential to include organizational and management culture.[76] Figure 1 describes that the civil and

---

[70] Herbert Lin, 2012, *Operational Considerations in Cyber Attack and Cyber Exploitation,* in Derek S. Reveron (ed), *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* Washington D.C.: Georgetown University Press, p.39

[71] Sun Haiyong, 2019, *U.S – China Tech War: Impacts and Prospects, China Quarterly of International Strategic Studies, Vol. 5, No. 2, 197–212*

[72] *Ibid.,* p.199

[73] *Ibid*

[74] Robert Sheldon and Joe Mcreynolds, 2015, *Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias,* in Jon R. Lindsay, Tan Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domains,* New York: Oxford University Press, p.188-189

[75] Tai Ming Cheung, 2009, *Fortifying China: The Struggle to Build a Modern Defense Economy*, Ithaca, NY: Cornell University Press

[76] *Ibid.,* p.197

military entities have numerous points of potential intersection:

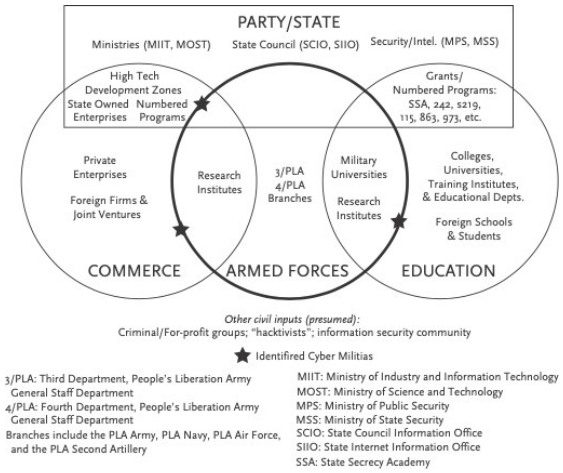

Figure 1. *Civil-Military Integration and Chinese Computer Network Operations*[77]

[77] Robert Sheldon and Joe Mcreynolds, *Op.Cit.,* p.190-191

In the 1990s, two People Liberation Army (PLA) air force officers have identified that the U.S military system was dependent on ICT, and PLA sought to exploit it.[78] The advancement of ICT in China led the PLA to effectively engaged in integrated network electronic warfare *(wangdian yiti zhan).* The Liberation Army Daily described the new electronic offensive capability in an article as follows."

> "In future hi-tech warfare, offensive operations will often necessitate pre-emptive destruction of the enemy's integrated battlefield command-and-control systems and warfare networks. Moreover, to attack its state or military communications hubs, financial centers, and C4ISER systems to affect the enemy's strategic decision-making directly "[79]

In regards to Huawei, it is believed that Huawei has closed ties with PLA. The relation includes cyber-related research and development funding from PLA.[80] Hence, the allegation of Huawei as the technological long arm of the China Communist Party.

The process of securitizing the technological adversary between China and the U.S under the Trump administration began in 2017 with the issuance of the National Security Strategy (NSS) Report proposing imposing trade sanctions on China and calling for relevant legislative measures.[81] Moreover, in November 2018, the U.S. Department of Commerce, via the Bureau of Industry and Security (BIS), targeted China's high-tech industrial planning by identifying emerging technologies essential to U.S. national security and listing 14 "representative technology categories."[82] It also included the innovative technological achievements produced by the R&D branches set up by Chinese enterprises in the United States in the scope of control.

Later in 2019, the Congress passed the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019), a clause that demanding the Ministry of Defense to formulate a "whole-of-government strategy on China" and design complex policies toward China among all government departments. The White House will be the lead in formulating the strategy on China.[83] Later, the U.S. State Department, Department of Education, Department of Homeland Security, and Department of Justice have taken concerted measures to limit China's use of U.S. cutting-edge science, technology, education research resources. By any means, the U.S forced China to abandon its state-led high-tech industrial policy and technology transfer through trade sanctions, investment control, and restrictions on the exchange of technological personnel.[84]

The Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation accused China of pressuring U.S companies to transfer technology using its foreign ownership restrictions regulation. China also allegedly imposed substantial restriction on U.S. firms' investments and activities, directing and facilitating the systematic investment in the acquisition of U.S. companies and assets to obtain cutting-edge technologies and intellectual property and to generate large-scale technology transfer in critical industries, and conducting and supporting "theft" from the computer networks

[78] Nigel Inkster, 2012, *China in Cyberspace,* in Derek S. Reveron (ed), *Op.Cit.,* p.202
[79] *Ibid*
[80] *Ibid*
[81] Sun Haiyong, 2019, *Op.Cit.,* p.201
[82] *Ibid.,* p.202
[83] *Ibid,* p.201
[84] *Ibid*

of U.S. companies.[85] The U.S. government has repeatedly accused China of "stealing U.S. technologies," so it has since tightened the visa application examination for Chinese nationals. It controlled and monitored the mobilization of Chinese and technology personnel as well.

On May 15, 2019, President Trump signed the Executive Order on Securing the Information and Communications Technology and Services Supply Chain. The order gives the Federal Government the power to block U.S. companies from buying foreign-made telecommunications equipment deemed a national security risk.[86] However, the order is explicitly seen targeted Chinese enterprises, as the U.S. repeatedly argues that China's Government could force companies like Huawei to install backdoors in their equipment to spy on American networks. Following to it, the next day on May 16, 2019, BIS issued a final rule amending the Export Administration Regulations ("EAR") by adding Huawei and 68 of its non-U.S. affiliates (collectively "Huawei") to the Entity Control List, cutting off trade opportunities between Huawei and its U.S. suppliers of critical components.[87]

Finally, Secretary of State Mike Pompeo, on August 5, 2020, announced the Clean Network Program with five new efforts to ensure; (1) clean carrier: to ensure untrusted People's Republic of China carriers are not connected with U.S telecommunication networks, (2) clean store: to remove PRC's untrusted application from U.S. mobile apps stores, (3) clean apps: to prevent untrusted PRC smartphone manufactures from pre-installing or making available to download trusted apps in their app store, (4) clean cloud: to prevent U.S. citizen's sensitive personal information and businesses' intellectual property from being stored and processed on foreign adversaries companies such as Alibaba, Baidu, and Tencent, (5) clean cable: to ensure global undersea internet cables are not subverted for intelligence gathering by PRC. All efforts are all meant to "guarding the U.S. citizens' privacy and our companies' most sensitive information from aggressive intrusion by malign actors, such as the Chinese Communist Party (CCP)."[88]

Conclusion

The U.S. ban on China's technology and telecommunication companies is a successful securitization act of the Trump administration. The Executive and its apparatus, including the United States Department of States and Federal Communications Commission, play the role of securitization actors, strategically push the issue of China's cyber intrusion as a National Security concern by building a referent object argument that China's technology companies are multi-layered threat towards the individual, corporation, and the U.S. itself. ZTE and Huawei‘s telecommunication infrastructures are deemed as the gateway for the People’s Republic of China’s illegal data gathering of U.S. entities. Simultaneously, China’s Tiktok and WeChat are

[85] The White House*, Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation,* March 22, 2018, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/
Ibid., p.202-203

[86] The White House, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain,* May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

[87] Bureau of Industry and Security, *Export Administration Regulations (EAR),* May 16, 2019, https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019

[88] U.S. Department of State. *Announcing the Expansion of the Clean Network to Safeguard America’s Assets.* 5 August 2020. Retrieved 27 August 2020. https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

accused of doing political censoring and tools for China's potential misinformation campaign. Therefore, from the U.S. perspective, a radical measure toward China's cyber-espionage apparatus, namely China's technology enterprises, is needed and justified. The Trump administration has successfully steered U.S. public opinion to believe China is a significant threat to the U.S. According to the 2020 Pew Research Center poll, 62 percent of the U.S. population believes China as a threat to the U.S., a 14 percent rise from the poll conducted in 2018.[89]

Bibliography

Books

Barasso, John, Marry Fallin, and Virginia Foxx. 2016. *Republican Platform, 2016.* Cleveland: Consolidated Solutions.

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

Clausewitz, Carl von. *War.* In Michael Howard and Peter Paret. 1976. Princeton, NJ: Princeton University Press.

Inkster, Nigel. 2012. *China in Cyberspace.* In Derek S. Reveron (ed). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, D.C.: Georgetown University Press.

Kello, Lucas. 2017. *The Virtual Weapon and International Order.* U.S.: Yale University Press.

Kuhn, Thomas S., 1996. *The Structure of Scientific Revolutions* (3rd ed). Illinois: Univesity of Chicago Press.

Lin, Herbert. 2012. *Operational Considerations in Cyber Attack and Cyber Exploitation*. In Derek S. Reveron (ed). *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, D.C.: Georgetown University Press.

Middlemas, Keith, and John Barnes. 1969. *Baldwin: A Biography*, London: Weidenfeld & Nicolson.

Rattray, Greg. 2001. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press.

Reveron, Derek S., 2012. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, D.C: Georgetown University Press.

Schelling, Thomas. 1966. *Arms and Influence.* New Haven: Yale University Press.

Sheldon, Robert, and Joe Mcreynolds. 2015. *Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias*. In Jon R. Lindsay, Tan Ming Cheung, and Derek S. Reveron. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domains*. New York: Oxford University Press.

Singer, P, W., and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* NY: Oxford University Press.

Tai Ming Cheung. 2009. *Fortifying China: The Struggle to Build a Modern Defense Economy*. Ithaca, NY: Cornell University Press.

Journals

Kello, Lucas. 2013. *The Meaning of the Cyber Revolution: Perils to Theory and*

[89] Brendan Cole,*Poll Find Most Americans Think China is a Major Threat to the U..S.,* Newsweek, June 6, 2020. https://www.newsweek.com/china-pew-research-u-s-threat-1508329

Statecraft. International Security Vol.38, No.2. Fall 2013.

Sun Haiyong. 2019. *U.S – China Tech War: Impacts and Prospects*. China Quarterly of International Strategic Studies Vol. 5, No. 2, 197–212.

Valeriano, Brandon, and Ryan Manness. 2015. *The Coming Cyberspace: The Normative Argument against Cyberwarfare.* Foreign Affairs, May 13, 2015.

Online News and Journals

Bass, Dina. 2019. *Microsoft Says Trump Is Treating Huawei Unfairly*. Bloomberg, September 8, 2019. Retrieved August 27, 2020. https://www.bloomberg.com/news/articles/2019-09-08/microsoft-says-trump-is-treating-huawei-unfairly

Chaudhary, Archana, Ragini Saxena, PR Sanjai, and Saritha Rai. 2020. *China's Huawei, ZTE Set To Be Shut Out of India's 5G Trials.* Bloomberg August 14, 2020. Retrieved August 27, 2020. https://www.bloomberg.com/news/articles/2020-08-13/china-s-huawei-zte-set-to-be-shut-out-of-india-s-5g-trials?cmpid=socialflow-twitter-business&utm_source=twitter&utm_campaign=socialflow-organic&utm_content=business&utm_medium=social

Collins, Katie. 2020. *U.K. follows U.S. in banning Huawei from 5G network*. CNET July 14, 2020. Retrieved August 27, 2020. https://www.cnet.com/news/uk-follows-us-in-banning-huawei-from-5g-network/

Delaney, Robert. 2018. *U.S. slaps China's ZTE with 7-year components ban for breaching terms of sanctions settlement.* South China Morning Post April 16, 2018. Retrieved August 27, 2020. https://www.scmp.com/business/companies/article/2142002/us-slaps-zte-seven-year-components-ban-breaching-terms-sanctions

Emmott, Robin. 2018. *U.S. warns European allies not to use Chinese gear for 5G networks.* Reuters February 5, 2018. Retrieved August 26, 2020. https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG

Feng, Emily, and Amy Cheng. 2019. *China's Tech Giant Huawei Spans Much Of The Globe Despite U.S. Efforts To Ban It.* National Public Radio (npr.org) October 24, 2019. Retrieved August 27, 2020. https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it

Feng Zhaoyin and Joshua Cheetam. 2020. *Trump WeChat ban 'an unwelcome signal' for Chinese community.* BBC News August 10, 2020. https://www.bbc.com/news/world-asia-china-53686507

Financial Times. 2019. *Google warns of U.S. national security risks from Huawei ban.* Financial Times. Retrieved August 27, 2020. https://www.ft.com/content/3bbb6fec-88c5-11e9-a028-86cea8523dc2

Heater, Brian. 2020. *Trump adds another year to Huawei/ZTE ban.* TechCrunch May 15, 2020. Retrieved August 27, 2020. https://techcrunch.com/2020/05/14/trump-adds-another-year-to-huawei-zte-ban/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGhucOEibiuOrvFD8hkQP-q1yzfMhR8gyE1gAEB_BwhN0UALH7roB9mmbR8tMdpK0_gSLf8LZPijexF2o-vJsXgwFG2m3r_-zDa-J0GKtjE2EueF5IKMHyfGOr8u3ZM8L4ncglz9RAXQb6ir4Ee0I_lBr9sWhAMTwL9Xnuq8fvg&guccounter=2

Isaac, Mike, and Ana Swanson. 2020. *TikTok Sues U.S. Government Over Trump Ban.* The New York Times, August 24, 2020. Retrieved August 27, 2020. https://www.nytimes.com/2020/08/24/technology/tiktok-sues-us-government-over-trump-ban.html

Keane, Sean. 2019. *Huawei lays off hundreds of U.S. workers due to blacklisting.* CNET July 23, 2019. Retrieved August 17, 2020. https://www.cnet.com/news/huawei-lays-off-hundreds-of-us-workers-due-to-blacklisting/

Maurer, Tim. *The Case of Cyberwarfare.* Foreign Policy October 19, 2011 (https://foreignpolicy.com/2011/10/19/the-case-for-cyberwarfare/). Retrieved October 19, 2018.

Musli, Steven. 2018. *Huawei executive arrested in Canada at U.S. request.* CNET December 6, 2018. Retrieved August 26, 2020. https://www.cnet.com/news/huawei-executive-arrested-by-canadian-officials-at-us-request/

Ng, Alfred. 2019. *Senators introduce bipartisan bill to address Chinese tech concerns.* CNET January 4, 2019. Retrieved August 27, 2020. https://www.cnet.com/news/senators-introduce-bipartisan-bill-to-address-chinese-tech-concerns/

O'Harrow Jr, Robert. *Understanding Cyberspace is Key to Defending Against Digital Attacks.* The Washington Post June 2, 2012 (https://www.washingtonpost.com/investigations/understanding-cyberspace-is-key-to-defending-againstdigital-attacks/2013/06/03/d46860f8-ad58-11e4-9c91-e9d2f9fde644_story.html?noredirect=on&utm_term=.ce434bb7eac1). Retrieved October 20, 2018

Reichert, Corinne, and Marguerite Reardon. 2019. *Huawei says U.S. ban will 'significantly harm' American jobs, companies.* CNET May 16, 2019. Retrieved August 27, 2020. https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-american-companies-jobs/

Reichert, Corinne. 2020. *U.S. finds Huawei has backdoor access to mobile networks globally, report says.*CNET February 12, 2020. Retrieved August 27, 2020. https://www.cnet.com/news/us-finds-huawei-has-backdoor-access-to-mobile-networks-globally-report-says/

Reichert, Corinne. 2020. *Huawei is backed by Chinese military, Trump administration finds.* 2020. CNET June 24, 2020. Retrieved August 27, 2020. https://www.cnet.com/news/huawei-is-backed-by-chinese-military-trump-administration-reportedly-finds/

Riley, Michael. *How Russian Hackers Stole the NASDAQ.* Bloomberg July 22, 2014. (https://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq). Retrieved October 20, 2018.

Schmitt, Eric, and Tom Shanker. *U.S. Debated Cyberwarfare in Attack Plan on Libya.* The New York Times October 17, 2011. (https://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1&hp) Retrieved October 19, 2018

Sherlock, Tracy, and Dan Bilefsky. 2020. *Extradition of Huawei Executive Clears, a Major Legal Hurdle in Canada.* The New York Times May 27, 2020. Retrieved August 27, 2020. https://www.nytimes.com/2020/05/27/world/canada/huawei-extradition-meng-wanzhou.html

Soo, Zen. 2019. *Trump's Huawei ban will hit rural U.S. carriers the hardest as*

replacing equipment will cost 'millions'. South China Morning Post, March 4, 2019. Retrieved August 27, 2020. https://www.scmp.com/tech/enterprises/article/2188422/trumps-huawei-ban-will-hit-rural-us-carriers-hardest-replacing

Stolyar, Brenda, and Christian de Looper. 2018. *ZTE and the U.S.: Everything you need to know.* Digital Trends April 13, 2018. Retrieved August 27, 2020. https://www.digitaltrends.com/mobile/commerce-bans-zte-from-exporting-technology-from-the-us/

The Economist. 2010 *War in The Fifth Domain,* Economist.com July 1, 2010. Retrieved August 27, 2020. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

Venturebeat. 2020. *China asks U.S. to stop 'unreasonable suppression' of Huawei.* Venturebeat.com May 16, 2020. Retrieved August 27, 2020. https://venturebeat.com/2020/05/16/china-asks-u-s-to-stop-unreasonable-suppression-of-huawei/

Venturebeat. 2020. *FCC finalizes Huawei and ZTE ban, citing threats to U.S. security*. Venturebeat.com June 30, 2020. Retrieved August 27, 2020. https://venturebeat.com/2020/06/30/fcc-finalizes-huawei-and-zte-ban-citing-threats-to-u-s-security/

Government Documents

Bureau of Industry and Security. *Export Administration Regulations (EAR*). May 16, 2019. Retrieved August 26, 2020. https://www.bis.doc.gov/index.php/all-articles/17-regulations/1555-addition-of-certain-entities-to-the-entity-list-final-rule-effective-may-16-2019.

European Commission. *Secure 5G networks: Commission endorses E.U. toolbox and sets out next steps.* January 29, 2020. Retrieved August 25, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

Petitions. *WeChat Should Not Be Banned.* The White House July 14, 2020. https://petitions.whitehouse.gov/petition/wechat-should-not-be-banned

The White House. *National Cyber Strategy 2018.* September, 2018. Retrieved August 27, 2020. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House. *National Security Strategy 2002.* September 17, 2002. Retrieved August 27, 2020. https://nssarchive.us/wp-content/uploads/2020/04/2002.pdf

The White House. *National Security Strategy 2006.* March, 2006. Retrieved August 27, 2020. https://nssarchive.us/wp-content/uploads/2020/04/2006.pdf

The White House. *National Security Strategy 2010.* May, 2010. Retrieved August 27, 2020. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

The White House. *National Security Strategy 2015.* February, 2015. Retrieved August 27, 2020. https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf

The White House. *National Security Strategy 2017.* December, 2017. Retrieved August 27, 2020. http://nssarchive.us/wp-content/uploads/2020/04/2017.pdf

The White House. *Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation.* March 22, 2018. Retrieved August 27, 2020. https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-

united-states-related-section-301-investigation/

The White House. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. May 15, 2019. Retrieved August 26, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

U.S. Department of Homeland Security. *U.S Department of Homeland Security Cybersecurity Strategy* May 15, 2018. Retrieved August 27, 2020. https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

U.S. Department of State. *Announcing the Expansion of the Clean Network to Safeguard America's Assets.* August 5, 2020. Retrieved August 27, 2020. https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

U.S. Department of State. *Executive Order on Addressing the Threat Posed by TikTok.* August 6, 2020. Retrieved August 27, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

U.S. Department of State. *Executive Order on Addressing the Threat Posed by WeChat*. August 6, 2020. Retrieved August 27, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/