5

Yea or Nay on Huawei? Altering the Balance of the 5G Technology War in Europe

Jefferson T. STAMP

Abstract: Although the potential security threat posed by Huawei's 5G technology has been under review for more than a year, Europe still lacks a unified response. The indecision is due in part to NATO's inability to address technology-based security issues that arise from international trade. To combat European ambivalence, the U.S. strategy has been to render Huawei an unreliable vendor in 5G development through the enforcement of export controls. In effect, the U.S. is using its hegemonic power in the international trading system to coerce European countries into an emerging technology-based security regime in opposition to the Chinese surveillance state. The research presented herein explores Huawei's technological disruption in the geopolitical context of strategic information warfare and examines how these factors color the current debate. The research demonstrates that, when making their ultimate decision on Huawei's 5G technology, European countries should consider the impact of technological disruption and strategic information warfare on the integrity of the international system as well as the importance of retaining sovereignty over critical infrastructure in the maintenance of their democratic societies and values.

Keywords: telecommunications, Huawei, 5G, technological disruption, strategic information warfare, surveillance, security, intelligence, NATO, export controls, hegemony, geopolitical

Introduction

European countries have been reviewing the security threat posed by Huawei's 5G technology for more than a year[362]. Of course, a quick 5G rollout using Huawei's telecommunications equipment could provide dramatic economic benefits. In the Information Age, efficient communication of large amounts of data is the key to generating wealth from data-driven goods and services[363]. Representing the next generation in data transmission capability[364], "5G could be the start of another round of innovation and growth similar to what we saw with the arrival of the internet…."[365]. As the current leader and cheapest supplier of 5G technology[366], Huawei is well-positioned to develop 5G infrastructure throughout the world[367]. On the other hand, if Huawei is restricted from 5G development, "European politicians fear falling further behind…."[368]. They also fear retaliation from China banning European products from the lucrative Chinese market[369]. Thus, the pragmatic approach has been to manage the potential security risks associated with utilizing Huawei's 5G technology without sacrificing the economic benefits.

---

[362] Saqib Shah, Liz Thomas and Cat Weeks, "Europe lacks a unified approach to Huawei despite yearlong assessments", *S&P Global Market Intelligence*, July 27, 2020, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/europe-lacks-unified-approach-to-huawei-despite-yearlong-assessments-59602291, (accessed August 8, 2020).

[363] James Lewis, "Can Telephones Race? 5G and the Evolution of Telecom Part I", *Center for Strategic International Studies*, (2020): 3.

[364] "Mobile wireless technology has evolved over four generations: voice calls in the 1980s (1G), messaging in the 1990s (2G), limited multimedia, text and internet data in the late 1990s and early 2000s (3G), and true data with dynamic information access and variable devices in the late 2000s (4G and LTE)". Andrea Gilli, "NATO & 5G: what strategic lessons?", *NATO Defense College*, no. 13 (July 2020): 1, https://www.jstor.org/stable/resrep25095, (accessed August 6, 2020).

[365] Ibid.

[366] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant", *Council on Foreign Relations*, August 6, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant (1/12, 8/12), (accessed August 23, 2020).

[367] "Huawei and 5G – The European Theatre", *The Economist*, July 18, 2020, 16.

[368] Ibid.

[369] Id., 17 ("Chinese reprisals against countries chucking out Huawei can be expected…".).

From a security analyst perspective however, it is Europe's ambivalence which itself presents the strategic lesson[370]. As pointed out by Andrea Gilli of the NATO Defense College, "this is the first time since the end of World War II that a leader of a key technology is neither an Ally nor a NATO/western country."[371]. Europe's lack of unity on Huawei reflects two competing technology paradigms; one that is focused on technology-based economic development grounded in globalism and free trade, while the other is focused on an emerging bipolar and technology-based security regime. The tension between these two paradigms highlights a shortcoming in NATO's limited construction as a "military alliance of democracies which was not designed to deal with trade policy, industrial leadership and market competition in the world of high-tech."[372]. The result has been the lack of a unified position after more than year of assessing the security threat.

Given the lack of a unified response by European countries, the containment of Huawei is now being driven by the United States as the hegemonic power in the international trading system. Specifically, the U.S. has imposed export controls which siphon Huawei's supply chain of critical U.S. technology such as semiconductors[373]. "Without U.S. technology, Huawei will be hard-pressed to make 5G infrastructure products…"[374].

The U.S. trade restrictions will no doubt force the Chinese government to develop its own internal supply chains. In this respect, "[e]xport controls on chips and chip-manufacturing might well have diminishing returns. A lack of competition from Western technology could simply help China build its industry in the long run."[375]. The U.S. export controls may also be

---

[370] Gilli, "NATO & 5G: what strategic lessons?", 4.

[371] Ibid., 3.

[372] Ibid., 4.

[373] Michael R. Pompeo, U.S. Secretary of State, "The United States Protects National Security and the Integrity of 5G Networks", U.S. Department of State, May 15, 2020, https://www.state.gov/the-united-states-protects-the-national-security-and-the-integrity-of-5g-networks (1/4), (accessed July 25, 2020).

[374] James Lewis, "Can Telephones Race? 5G and the Evolution of Telecom Part I", 4.

[375] Ben Buchanan, "The U.S. has AI Competition All Wrong", *Foreign Affairs*, August 7, 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-07/us-has-ai-competition-all-wrong (5/9).

undermined from alternative sources in competing nations[376]. For these reasons, Bown argues that successful export controls against Huawei should be "multilateralized" so that other countries cooperate in restricting substitute supplies to Huawei[377]. "However, the supply chain for telecom will depend on semiconductors and specialized software, all areas where the United States has a substantial lead."[378]. Thus, the unilateral approach by the U.S. may be still successful in at least temporarily stifling Huawei's drive to develop the world's 5G infrastructure because the export controls are focused on a supply chain that the U.S. currently dominates.

The immediate aim of this U.S. policy is seemingly to coerce Europe into an alignment of democratic countries within an emerging bipolar techno-security regime. If that is the case, the decision over Huawei's 5G technology is one to be made in the current geopolitical context; *i.e.*, will European nations utilize and rely upon the lesser developed technology from a democratic source committed to the relatively free flow of data and thereby maintain sovereignty over their telecommunications network, or will they utilize and rely upon the expedient technology from a communist source that is undergirding the Chinese surveillance state and projecting the power of the Chinese Communist Party?

In order to determine how best to answer the question about Huawei, the following research focuses on a brief history of technological disruption and strategic information warfare, the resulting 5G security threat in light of Huawei's role within China's surveillance state and the effect of U.S. export controls on the balance of the 5G technology war.

---

[376] Chad P. Bown, "Export Controls: America's Other National Security Threat", *Duke Journal of Comparative & International Law*, 30 (2020): 291–292, https://www.scholarship.law.duke.edu/djcil/vol30/iss2/4, (accessed August 1, 2020).

[377] Ibid., 291.

[378] Lewis, 8.

Brief History of Technological Disruption and Strategic Information Warfare

One of the greatest lessons in human history is the importance of technology in military affairs and how technological revolutions can redefine the world order. At the beginning of this century, Max Boot explained how advances in technology affect the international system: "Over the last 500 years, the fate of nations has been increasingly tied to their success, or lack thereof, in harnessing revolutions in military affairs. These are periods of momentous change when new technologies combine with new doctrines and new forms of organization to transform not only the face of battle but also the nature of the state and the international system."[379].

The Mongols, as Boots highlights, maintained the "mightiest military forces" until the 15th century when they failed to "keep pace with the spread of gunpowder weapons and the rise of centralized governments that used them."[380]. Implicit in the centralization of government control was the ability to harness national communications such as the semaphore system of telegraphs in Revolutionary and Napoleonic France[381]. Schofield asserts, "From the outset, the prime purpose [of this communications network] was military."[382]. However, Dumas famously depicted how such a network could be compromised to spread disinformation and cause a financial panic in *The Count of Monte Cristo*[383].

---

[379] Max Boot, "Are we the Mongols of the Information Age?", *Los Angeles Times*, October 29, 2006, https://www.latimes.com/archives/la-xpm-2006-oct-29-op-boot29-story.html (1/5), (accessed August 4, 2020).

[380] Ibid.

[381] Patrice Flichy, "The Birth of Long Distance Communication. Semaphore Telegraphs in Europe", *Réseaux. The French Journal of Communication*, 1.1 (1993): 81–101, https://www.persee.fr/doc/reso_0969-9864_1993_num_1_1_3272, (accessed August 9, 2020).

[382] Hugh Schofield, "How Napoleon's semaphore telegraph changed the world", *BBC News Magazine*, June 17, 2013, https://www.bbc.com/news/magazine-22909590 (4/16), (accessed August 15, 2020).

[383] David Alan Grier, "What the Count of Monte Cristo Can Teach Us About Cybersecurity", *IEEE Spectrum*, January 25, 2018, https://spectrum.ieee.org/tech-talk/telecom/security/what-the-count-of-monte-cristo-can-teach-us-about-cybersecurity, (accessed August 17, 2020).

"Historically", Gilli argues, "communications have been at the centre of geopolitical competition among countries."[384]. By the 20th century, one of the first examples of "strategic information warfare" was the British plan "to cut German undersea cables across the world."[385]. Taking advantage of its control over a global network of colonial outposts, "Britain's strategy was to deprive Germany of its outside communications and force communications from German cables onto British-controlled wires, where they could be collected and decrypted."[386]. As a result, Britain was able to "use cable cutting and censorship as strategic resources in World War I."[387].

Subsequently, "Radio itself altered the conceptualization of international communications. Radio enabled governments to control their own infrastructure."[388]. This new technology neutralized British hegemony over communications, and combined with electronics, helped set the stage for the "Information Revolution" after World War II. Computer technology, in turn, ushered in a new world order. Boot points out, "The Soviet Union had no Silicon Valley and could not compete with the United States in incorporating the computer into its economic or military spheres. U.S. prowess at waging war in the Information Age was showcased in the 1991 Persian Gulf War, which, along with the collapse of the Soviet empire, left the United States standing alone as a global hegemon."[389].

---

[384] Gilli, "Nato and 5G: what strategic lessons?", 2.

[385] Calder Walton, "China Will Use Huawei to Spy Because So Would You", *Foreign Policy*, July 14, 2020, https://foreignpolicy.com/2020/07/14/britain-boris-johnson-china-will-use-huawei-to-spy-because-so-would-you (3/14), (accessed July 15, 2020).

[386] Ibid.

[387] Jill Hills, *The Struggle for Control of Global Communication*, (University of Illinois Press, 2002), 286, https://www.jstor.org/stable/10.5406/j.ctt2ttcks.13, (accessed August 6, 2020).

[388] Ibid., 288.

[389] Boot, (2/5).

The 5G Security Threat posed by China's Huawei in Strategic Information Warfare

With the advent of the computer and the Internet, the age of wireless telecommunications presents a new set of opportunities for strategic information warfare. At the same time, history's lessons for nations to maintain control of their information technology infrastructure, provides a guide for insulating against these modern security threats.

A recent study by Ainikki Riikonen argues, "Information architecture–the structures of technology that collect and relay information worldwide–is innately connected to power projection."[390]. Starting from this thesis, Riikonen warns that China has been the most innovative in this area and is doing so in a manner that threatens the very foundation of democratic governance. Specifically, "the PRC will weaponize connectivity and employ technologies that maximize the CCP's agency over the availability and flow of information. Agency over information architecture is a potent tool for states in understanding and shaping the international environment and in winning both political and military confrontations."[391].

When assessing agency over information architecture, there are at least three spheres of vulnerability that result from the use of Huawei's 5G equipment in a telecommunications system. First, "tech-enabled connectivity" is what is viewed by China as "the back bone of U.S. military superiority" because technology now provides the infrastructure for all U.S. military operations, including command and control[392]. By focusing on gaining an edge in information technology infrastructure, China could potentially undermine U.S. operations by cutting the cyberspace "cables" upon which all U.S. communications depend.

For at least the past decade, the U.S. has formally recognized the threat to "commercial information technology, or IT, infrastructure" as a "new

---

[390] Ainikki Riikonen, "Decide, Disrupt, Destroy", *Strategic Studies Quarterly*, 13, no. 4, (Winter 2019): 122, https://www.jstor.org/stable/10.2307/26815049, (accessed July 25, 2020).

[391] Ibid., 123.

[392] Ibid.

asymmetry in future warfare."[393]. Digital war games conducted by Australia in early 2018 have similarly exposed China's "offensive potential" from having "access to equipment installed in the 5G network."[394]. As Sanger and Brooks discuss, "the struggle over 5G is about far more than trade or technical advantage. It is about the power to control a nation's infrastructure–and, in time of conflict, to cut off an adversary's ability to communicate. And that makes the geopolitics as important as the technology."[395].

Given this vulnerability, it is highly unlikely that U.S. forces would undertake significant operations in defense of any NATO country with a Huawei-based telecommunications infrastructure. To do so would effectively cede China the power to cut off all communications in a time of conflict or crisis. Consequently, European countries "could inject serious risk" to "defense cooperation" with the United States if they allow Huawei to build their 5G telecommunications network[396].

The second sphere of vulnerability concerns espionage. Walton explains that "Huawei's presence on [a] 5G network could allow Beijing to conduct economic espionage … [and] also collect ostensibly nonsensitive bulk data…."[397]. This bulk data may inadvertently reveal more sensitive information from "defense, security and intelligence services."[398]. Given this vulnerability, the U.S. has threatened to withhold intelligence from any NATO country that uses Huawei technology in its telecommunications infrastruc-

---

[393] Cheryl Pellerin, "Lynn: cyberspace is new domain of warfare", Armed Forces Press Service, CENTCOM (October 19, 2010), https://centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/884164/lyn-cyberspace-is-new-domain-of-warfare (1/4), (accessed August 15, 2020).

[394] Casell Bryan-Low, Colin Packham, David Lague, Steve Stecklow and Jack Stubbs, "Hobbling Huawei: Inside the U.S. war on China's tech giant", *Reuters*, May 21, 2019, https://www.reuters.com/investigates/special-report/huawei-usa-campaign (3/15), (accessed July 25, 2020).

[395] David A. Sanger and Mary K. Brooks, "Battlefield 5G: Are the U.S. and China destined for a forever-war over network control?", *Wilson Quarterly* (Spring 2020), https://www.wilsonquarterly.com/who-writes-the-rules/battlefield-5g (2/11), (accessed August 22, 2020).

[396] Mark T. Esper, U.S. Secretary of Defense, "As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference", U.S. Department of Defense, February 15, 2020, https://defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security (6/8), (accessed August 15, 2020).

[397] Walton, "China Will Use Huawei to Spy Because So Would You", (13/14).

[398] Ibid.

ture. As explained by U.S. Defense Secretary Esper: "Reliance on Chinese 5G vendors … could render our partners' critical systems vulnerable to disruption, manipulation and espionage. It could also jeopardize our communication and intelligence sharing capabilities, and by extension, our alliances."[399].

In addition, the 5G data stream controlled by Huawei could provide China information from virtually all devices connected via the Internet of Things, disclosing industrial processes and an infinite array of data points that will improve China's Artificial Intelligence and other technical applications. "The true scale of the threat posed by 5G Huawei hardware becomes clear when we consider how it could be combined with billions of internet-enabled devices, sensors, and gadgets in households, offices, and infrastructure, most of which are unsecured and whose owners may not even know are networked. They would effectively constitute billions of backdoors…."[400].

Utilizing this massive database, "Chinese scientists could use a rapidly developing methodology called 'social network analysis,' which reveals nonobvious relationships between places and people, for intelligence targeting…."[401]. The potentially limitless cache of data and new applications from Huawei's 5G networks would provide China a several degrees of magnitude advantage both in military and industrial decision-making, and also present China with a perfect platform for spreading disinformation.

The third sphere of vulnerability is in the area of cyberattacks. In November 2019, the European Union Agency for Cybersecurity (ENISA) issued its report on the "Threat Landscape for 5G Networks", detailing ENISA's "threat assessment for the 5th generation of mobile telecommunications networks." Among the comprehensive list of enumerated threats, one threat stands out – the threat from "nation states" and the relationship they may have to 5G vendors.

---

399 Esper, "Munich Security Conference", (7/8).

400 Walton, (13/14).

401 Ibid.

The ENISA report concludes: "It is indisputable that vendors of 5G components – just like any other technology vendor – are in a better position to cause devastating attacks to the operation of self-developed components, especially when governments influence them. Given the importance of 5G to the sovereignty of nation-states, they will probably be a target of state-sponsored attacks."[402]. While no vendor was singled out, the report unmistakably describes the cyber-security threat posed by the largest 5G vendors in the world, including China's Huawei. Only upon review of Huawei's role in China's surveillance state can the threat be fully appreciated.

Huawei's role in the Surveillance State and China's policy of Military-Civil Fusion

At the heart of the emerging Chinese surveillance state is the collection of data by technology companies like Huawei. In an article by the Epoch Times in 2018, it was reported that Huawei "plays a pivotal role in establishing high-tech totalitarianism across China's cities [and] provinces."[403]. Specifically, Huawei has assisted in the Chinese Communist Party's creation of an "urban digitization scheme" called "China Skynet" in order to "surveil 1.4 billion Chinese people, suppress political opponents, and persecute minorities."[404].

It was further reported that the Chinese surveillance system includes more than 170 million cameras with more than 400 million cameras planned for installation over a period of three years[405]. For its part, Huawei led the development of the facial recognition software that is used by the govern-

---

[402] Marco Laurenco and Louis Marinos, "ENISA Threat Landscape for 5G Networks", *European Union Agency for Cybersecurity*, (November 2019): 72, https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks, (accessed August 1, 2020).

[403] He Jian, "Huawei and the Creation of China's Orwellian Surveillance State", *The Epoch Times*, December 24, 2018, updated January 8, 2019, https://www.theepochtimes.com/huawei-and-the-creation-of-chinas-orwellian-surveillance-state_2747922.html (1/8), (accessed July 25, 2020).

[404] Ibid., (2/8).

[405] Ibid.

ment to keep track of every individual citizen[406]. Huawei technology has also been used in the massive surveillance and detention of the Uyghurs in the Xinjiang province[407]. Based on omnipresent technological surveillance and the perpetual accumulation of personal data, a "citizen score" rates the entire population on their obedience to the state[408].

The participation of Huawei and other technology companies in massive state surveillance raises questions about the role of such companies in society[409]. Are these profit-making ventures merely assisting the government in the mass surveillance of the general population for some public good such as the reduction of terrorism? Or are these companies actually extensions of the Chinese Communist Party embracing an integral role in the maintenance of power and oppression over the general population? The history of Huawei strongly suggests the latter is the case.

From its founding in the 1980's, Huawei "has had ties with the People's Liberation Army (PLA) and other security apparatuses of the Chinese party-state."[410]. Umback's study confirms that: "Huawei has received strong political support from the Chinese party-state since its infancy, and that support proved instrumental in its initial survival and subsequent global expansion. Today, it occupies a key position in major initiatives of the party-state, including the 'Digital Silk Road' component of the Belt and Road Initiative and the strategy of 'civil-military fusion.'"[411].

In 2016, Chinese President Xi Jinping adopted "civil-military fusion" as a formal policy to enhance "the development of dual-use technology and [to] integrate existing civilian technologies into the arsenal of the People's

---

406 Ibid.

407 Ibid., (4–5/8).

408 Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone", *The Atlantic*, February 2, 2018, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/ (2/6), (accessed July 18, 2020).

409 Ibid., (3/6).

410 Rick Umback, "Huawei and Telefunken: Communications enterprises and rising power strategies", *Strategic Insights*, (Australian Strategic Policy Institute, 2019): 7, http://www.jstor.com/stable/resrep23012, (accessed August 6, 2020).

411 Ibid., 6.

Liberation Army."[412]. Moreover, China's National Intelligence Law, adopted the following year, requires all business organizations to "support, cooperate with and collaborate in national intelligence work."[413]. Pursuant to this legal authority, Chinese companies simply do not "have the option of turning down government requests to share technology."[414]. Yi-Zheng Lian points out, "Spying for the state is a duty of the citizens and corporations of China under the law, much like paying taxes."[415]. Considering Huawei's history and the policy of civil-military fusion, Huawei is inescapably intertwined within the Chinese military-industrial-complex. Accordingly, the U.S. Defense Department has identified Huawei as being owned or controlled by China's military[416].

Faced with the reality of Huawei's connections to the Chinese surveillance state, European countries must consider the security implications of relying on Huawei's 5G technology in the context of geopolitics and strategic information warfare. First, opting for Huawei is tantamount to placing control of the state's 5G networks in the hands of the Chinese government. Under this scenario, the telecommunications and data flows supporting the entirety of society could be surveilled, manipulated and undermined by China for political and military purposes. Reliance on Huawei in this manner is, therefore, fundamentally at odds with European democratic values and ultimately jeopardizes the very sovereignty of targeted democratic states. Accordingly, an analysis of the hybrid aspects of high technology must constitute part of the calculus of any nation state when assessing the security threat from Huawei. Democratic governments in particular,

---

[412] Anja Manuel and Kathleen Hicks, "Can China's Military win the Tech War? How the United States Should-and Should Not-Counter Beijing's Civil-Military Fusion", *Foreign Affairs*, July 29, 2020, https://www.foreignaffairs.com/articles/united-states/2020-07-29/can-chinas-military-win-tech-war (2/12), (accessed July 29, 2020).

[413] Maizland and Chatzky, "Huawei: China's Controversial Tech Giant", (6/12).

[414] Ibid., (3/12).

[415] Yi-Zheng Lian, "Where Spying is the Law", *The New York Times*, March 13, 2019, https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html (1/2), (accessed August 23, 2020).

[416] Tony Capaccio and Jenny Leonard, "Huawei on List of 20 Chinese Companies that Pentagon Says Are Controlled by People's Liberation Army", *Time*, June 25, 2020, https://time.com/5859119/huawei-chinese-military-company-list, (accessed July 25, 2020).

given their relative freedom and openness, are the most vulnerable to the types of subversion and sabotage of telecommunications networks that would be possible under the Orwellian world interposed by China through Huawei's 5G technology.

The Use of U.S. Export Controls to Alter the Balance of the 5G Technology War

Notwithstanding the security concerns outlined above, democratic countries in Europe have been reluctant in making the switch from Huawei[417]. "While telecoms operators in the bloc have called for clarity on government policies towards Huawei", Shah, Thomas and Weeks argue, "the region is still highly divided, with almost an equal number of countries excluding and including the Chinese company from 5G rollouts."[418].

One reason for the division in Europe is that the United States itself does not have an exemplary record for respecting the sanctity of international telecommunications security. Thus, "at its most basic level, the U.S. versus Huawei fight is also a raw geopolitical competition between two superpowers with advanced signals intelligence capabilities and extremely pervasive global surveillance networks."[419]. The U.S. response seems to be that western intelligence agencies, unlike China's security apparatus, are "beholden to democratic legal systems and respect for human rights and political speech."[420]. While not exactly reassuring to the skeptics and cynics, there is no denying an element of *realpolitik* as a critical factor in the debate. In effect, the U.S. is leveraging its position in the current world order as the ultimate safe refuge for democratic institutions and the people who yearn for them.

---

[417] Shah, Thomas and Weeks, "Europe lacks unified approach to Huawei despite yearlong assessments", (1/4).

[418] Ibid., (2/4).

[419] Garret M. Graff, "Could Trump Win the War on Huawei–and Is Tik Tok Next?", July 14, 2020, https://www.wired.com/story/could-trump-win-the-war-on-huawei-and-is-tiktok-next (10/15), (accessed July 25, 2020).

[420] Ibid.

When viewed in this light, it is not surprising that the U.S. was able to gain its initial foothold for restrictive commitments against Huawei in a group of three Eastern European countries–Romania, Poland and Estonia[421]. As such, Brinza found that the U.S. security guarantee paved the way for a 5G solution among these allies that will be completely Huawei-free: "While China may hold leverage in the form of some unfulfilled investments, the United States is the security guarantee that can keep Central and Eastern Europe free from the perceived Russian threat. That is why the United States succeeded in signing its first anti-Huawei memorandum of understanding in Eastern, not Western, Europe."[422].

Western European countries, including the E.U. as a whole, have been more deliberative. In March 2019, the European Commission issued a voluntary recommendation for each European state to generically assess the cybersecurity risks of 5G networks, including "the overall risk of influence by a third country…."[423]. While talks were anticipated to continue throughout the year, it was clear from the Commission's recommendation that "Washington failed to get its Huawei ban…."[424]. Instead, the plan was to review the issues and "demand stricter security measures on telecoms vendors by the end of the year."[425].

The year lapsed with Prime Minister Boris Johnson's decision in January 2020 which "approved a substantial if clearly demarcated role for Huawei in Britain's 5G telecoms infrastructure."[426]. The decision was justified on the grounds that established procedures would safeguard Britain's "core" infrastructure, and also that Huawei's equipment could be relegated to the

---

[421] Andreea Brinza, "How Russia helped the United States fight Huawei in Central and Eastern Europe", *War on the Rocks*, March 12, 2020, https://www.warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe (2/8), (accessed July 25, 2020).

[422] Ibid., (7/8).

[423] European Commission, "Commission Recommendation – Cybersecurity of 5G networks", March 26, 2019, 4, https://www.ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks, (accessed August 1, 2020).

[424] Laurens Cerulus, "7 takeaways on the EU's Huawei plan", *Politico*, March 26, 2019, https://www.politico.eu/article/europe-huawei-7-takeaways-on-plan (3–4/6), (accessed August 8, 2020).

[425] Ibid., (2/6).

[426] "Huawei and 5G – The European Theatre", *The Economist*, July 18, 2020, 15.

"non-core" components of the network[427]. In this manner, "Britain could get its 5G systems up and running considerably sooner, and cheaper, than would otherwise be possible."[428].

Having been rejected by its closest of allies, the U.S. was forced to employ its hegemonic power in the international trading system to coerce its democratic brethren into excluding Huawei. On May 15, 2020, the U.S. announced it was adopting a set of stringent export controls barring the sale or transfer of any U.S. technology to Huawei[429]. This new restriction is intended to apply globally. As explained by U.S. Secretary of State Pompeo: "It also imposes U.S. export controls on countries that use U.S. technology or software to design and produce semiconductors for Huawei. Companies wishing to sell certain items to Huawei must now obtain a license from the United States government."[430].

With its supply chain now under siege, Huawei has quickly become an unreliable vendor. As reported by NPR: "Analysts say this latest move likely spells a death knell for Huawei's global ambitions by freezing out the Chinese company from fundamental semiconductor technology and by raising the costs for hundreds of countries that were relying on Huawei components for their 5G expansion plans, including many in Europe."[431]. According to Alex Capri at the National University of Singapore, this is a "watershed moment because it's the beginning of an emerging technonationalist reality."[432]. A former British diplomat acknowledged the geopolitical reality: "There was a bit of a checkmate by the U.S."[433].

---

[427] Ibid.

[428] Ibid.

[429] Michael R. Pompeo, U.S. Secretary of State, "The United States Protects National Security and Integrity of 5G Networks", U.S. Department of State, May 15, 2020, https://www.state.gov/the-united-states-protects-national-security-and-the-integrity-of-5g-networks (1/4), (accessed July 25, 2020).

[430] Ibid.

[431] Emily Feng, "The Latest U.S. Blow to China's Huawei Could Knock Out Its Global 5G Plans", *NPR*, May 28, 2020, https://www.npr.org/2020/05/28/862658646/the-latest-u-s-blow-to-chinas-huawei-could-knock-out-its-global-5g-plans (2/10), (accessed July 27, 2020).

[432] Ibid., (3/10).

[433] Adam Satariano, Stephen Castle and David E. Sanger, "U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates", *The New York Times*, July 14, 2020, https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html (2/3), (accessed August 17, 2020).

The U.S. "decoupling" from the China matrix will inevitably force every democratic country in Europe to make a "binary choice" between the two technological paradigms, resulting in a "bifurcation of the global economy."[434]. On July 14, 2020, two months after the U.S. imposition of global export controls on Huawei, the British government reversed its earlier decision and announced that it was banning Huawei equipment from its 5G networks[435]. Moreover, any currently installed Huawei equipment must be removed by 2027[436]. The reversal is estimated to delay Britain's implementation of 5G approximately two to three years with an estimated cost of about 2 billion pounds[437].

At the same time, Prime Minister Johnson is now proposing a "new institution" consisting of "an alliance of ten leading democracies–consisting of the G-7 countries plus Australia, India and South Korea and dubbed the 'D10'–to coordinate telecom policy and develop an alternative to China's market leader Huawei…."[438]. Thus, in an ironic twist, the new push for multilateralism in the fight against Huawei, which was originally viewed by some as a condition precedent for any successful enforcement of U.S. export controls, has actually been triggered by the unilateral action by the U.S.

While the story of this new multilateralism is still unfolding, it is fair to say that the U.S. export controls are beginning to alter the balance in the 5G technology war in Europe. As stated by U.S. Secretary of State Pompeo, "The tide is turning against Huawei as citizens around the world are waking up to the danger of the Chinese Communist Party's surveillance state."[439].

---

[434] Darren J. Lim and Victor Ferguson, "Conscious Decoupling: The Technology Security Dilemma", in *China Dreams*, Eds. Jane Golley, Linda Javin, Ben Hillman, Sharon Strange (ANU Press, 2020), 120.

[435] Satariano, Castle and Sanger, (1/3).

[436] "Huawei and 5G – The European Theatre", *The Economist*, July 18, 2020, 15.

[437] Ibid., 16.

[438] Edward Fishman and Siddharth Mohandas, "A Council of Democracies Can Save Multilateralism", *Foreign Affairs*, August 3, 2020, https://foreignaffairs.com/articles/asia/2020-08-03/council-democracies-can-save-multilateralism (2/10), (accessed August 3, 2020).

[439] Michael R. Pompeo, U.S. Secretary of State, "The Tide is Turning Toward Trusted 5G Vendors", June 24, 2020, https://www.state.gov/the-tide-is-turning-toward-trusted-5g-vendors (1/4) (accessed July 25, 2020).

Conclusion

The security challenge posed by Huawei in the development of 5G telecommunications networks concerns the potential vulnerabilities of democratic nations to high-tech surveillance and the loss of sovereignty over critical infrastructure. Because of Huawei's connections to the Chinese government, virtually all wireless communications and data transfers could be subject to the control of the Chinese surveillance state.

In response to European ambivalence on this issue, the U.S. strategy has been to render Huawei an unreliable vendor in 5G development through the enforcement of export controls. In effect, the U.S. is using its hegemonic power in the international trading system to coerce European countries into an emerging technology-based security regime in opposition to the Chinese surveillance state.

The research presented herein has explored Huawei's technological disruption in the geopolitical context of strategic information warfare and examined how these factors color the current debate. The research demonstrates that, when making their ultimate decision on Huawei, European countries should consider the impact of technological disruption and strategic information warfare on the integrity of the international system as well as the importance of retaining sovereignty over critical infrastructure in the maintenance of their democratic societies and values. When these considerations are taken into account, it seems clear that European countries should develop an alternative 5G telecommunications network, delink from the Chinese technology matrix and align with the U.S. in a new technology-based security regime.