ALTERNATE REALITIES: CRITICAL EVALUATION OF U.S. LEGAL SANCTIONS ON "COMMUNIST CHINESE MILITARY COMPANIES"

Colin Hawes & Grace Li*

Table of Contents

* Associate Professors at the University of Technology Sydney (UTS). The authors acknowledge a research grant from the Australia-China Relations Institute, UTS, and would also like to thank the careful reviewers and editors at the Tsinghua China Law Review.

ALTERNATE REALITIES: CRITICAL EVALUATION OF U.S. LEGAL SANCTIONS ON "COMMUNIST CHINESE MILITARY COMPANIES"

Colin Hawes & Grace Li

Abstract:

This paper examines the sanctions imposed on "Communist Chinese Military Companies" (CCMCs) by the Trump administration in 2020, and their 2021 modification by President Biden, which target Chinese companies in "defense and related materiel" and "surveillance technology" industries. The first part of the paper introduces key executive orders and relevant legal provisions. The second part of the paper provides a detailed analysis of successful court injunctions obtained by two Chinese companies, Xiaomi and Luokung, as well as their implications for the defects of the original CCMC process. Next, the paper evaluates the continued inclusion of several companies on the current list, from June 2021, casting doubt on how much President Biden's modified executive order would improve the inconsistent, if not arbitrary, decision-making process. The last part of the paper questions the underlying assumptions that sanctions introduced in such a hasty fashion would contain national security threats China posed to the U.S., make Chinese people better off, or establish the U.S. as a staunch defender of the rule of law.

Keywords: China, United States, sanctions, military companies

I. INTRODUCTION

When criticizing China, U.S. lawmakers and media commentators often picture the Chinese government, led by the Chinese Communist Party (CCP), as a rule breaker who acts in an arbitrary way without any respect for human rights and the rule of law. For example, in one of his 2018 remarks, former Vice President Mike Pence said:[1]

> At the turn of the 21st Century, America agreed to give Beijing open access to our economy, and bring China into the World Trade Organization. Previous administrations made this choice in the hope that freedom in China would expand in all forms – not just economically, but politically, with a newfound respect for classical liberal principles, private property, religious freedom, and the entire family of human rights… but that hope has gone unfulfilled.

And former Secretary of State Michael Pompeo furthered those criticisms in 2020:[2]

[1] Mike Pence, *Vice President Mike Pence's Remarks on the Administration's Policy Towards China*, HUDSON INSTITUTE (Oct. 4, 2018), https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018.

[2] Michael R. Pompeo, *Remarks at the Richard Nixon Presidential Library and Museum*: *Communist China and the Free World's Future* (Jul. 23, 2020), https://sv.usembassy.gov/secretary-michael-r-pompeo-

> We, the freedom-loving nations of the world, must induce China to change, … because Beijing's actions threaten our people and our prosperity. … We know that trading with China is not like trading with a normal, law-abiding nation. … The CCP is repeating some of the same mistakes that the Soviet Union made – alienating potential allies, breaking trust at home and abroad, rejecting property rights and predictable rule of law.

Whatever the merits of these criticisms of China, the underlying assumption remains that the governments of the "freedom-loving nations" led by the United States do respect the rule of law and would not abuse their powers to engage in arbitrary actions with scant legal justification.

This paper challenges this assumption by focusing on the recently imposed U.S. sanctions on "Communist Chinese Military Companies" (CCMCs). After introducing the context and recent expansion of these sanctions, the paper shifts gear to demonstrate how the initial list of CCMCs was issued without adequate research and was based on vague, if not false, interpretations of the underlying legislation, as evidenced by the inclusion of Chinese corporations that clearly did not have any military affiliations. While some of these corporations were removed from the most recent list following court challenges, the U.S. government has added other names. The scope of CCMCs has been broadened to such an extent that its original purpose of countering the Chinese military threat has been overlaid with an amorphous category involving surveillance by the Chinese government of its own people. Arguably, not only Chinese entities but also U.S. technology companies whose products may be used by Chinese police and security forces fall within the purview of sanctions. This government overreach can easily backfire. And despite the scope of the new definition, it is still unclear why several firms were listed, as no explanation or convincing evidence has been publicly disclosed to prove their affiliation with the Chinese military or police/security surveillance sector.

The arbitrary nature of this sanctions process, which has so far failed to follow basic rule of law principles, will be counter-productive. Combined with other recent, politically motivated sanctions by the U.S. against China, they supply ammunition for the Chinese government's propaganda system to claim that the U.S. is hypocritical, demanding higher rule of law standards from China than the U.S. can meet itself.[3]

---

remarks-at-the-richard-nixon-presidential-library-and-museum-communist-china-and-the-free-worlds-future/.

[3] For a selection of Chinese government responses to US sanctions, see: *China Criticizes US Missile Sanctions as Hypocrisy*, AP NEWS (Jan. 21, 2022), https://apnews.com/article/technology-business-united-states-beijing-china-aee573a2fd9b5acfb7372745c6a0b351; *China slams reported US sanctions on SMIC, other Chinese firms*, GLOBAL TIMES (Dec. 15, 2021), https://www.globaltimes.cn/page/202112/1241579.shtml; Associated Press, *China Criticizes US Moves to Expand Financial Sanctions*, US NEWS & WORLD REPORT, (Jul. 9, 2021), https://www.usnews.com/news/us/articles/2021-07-09/china-criticizes-us-moves-to-expand-financial-sanctions.

Although not the main focus of this paper, the expansion of these unilateral U.S. sanctions which now target Chinese corporations selling surveillance technology within Chinese territory, is in danger of breaching established principles of international law, especially the principle of non-interference in the internal affairs of other states under the United Nations Charter and related legal instruments.[4]

In the following sections, this paper will introduce relevant legal provisions, and analyze the successful court injunctions obtained by two companies on the original list, Xiaomi and Luokung, to demonstrate the defects of the CCMC process. Next, the paper will provide a breakdown of the Chinese companies that remain on the current list, as updated in June 2021, to show their diversity and the continuing lack of clarity about the criteria for including or excluding them. The conclusion will broaden the scope of analysis to question the effectiveness of such sanctions – especially how they have been implemented – and to challenge their underlying assumptions that these sanctions help to contain Chinese threats and improve the lives of Chinese people.

Unfortunately, due to space limitations, this paper cannot carry out an examination of the broader range of U.S. sanctions impacting Chinese corporations, including the Commerce Department's export bans on U.S. firms, restrictions on Chinese firms investing in the U.S. or acquiring U.S. technology businesses, and direct lawsuits against some Chinese firms like Huawei Technologies and ZTE Corporation, as well as extraterritorial pressure exerted on other countries to try to prevent Huawei and ZTE from doing business in their territories.[5] The plan is to address all these other types of sanctions in a separate paper.

II. WHAT IS THE LEGAL BASIS AND BACKGROUND CONTEXT FOR THE BLACKLISTS?

The primary legal basis for the U.S. government's actions against these companies is s.1237 of the National Defense Authorization Act (the "NDAA"), which dates back to 1998. The NDAA primarily focuses on authorizing U.S. government funding for its military forces, but it does include a few sections

[4] For detailed discussion of the international law principles, see: IRYNA BOGDANOVA, UNILATERAL SANCTIONS IN INTERNATIONAL LAW AND THE ENFORCEMENT OF HUMAN RIGHTS §2 (2022); and Julia Schmidt, *The Legality of Unilateral Extra-territorial Sanctions under International Law,* 27 J. CONFLICT & SEC. L. 53–81 (2022), https://doi.org/10.1093/jcsl/krac005.

[5] For various "entity lists" and sanctions policies aimed at Chinese firms, see U.S. Department of Commerce, *Entity List*, https://www.commerce.gov/tags/entity-list; U.S. International Trade Administration, *China: US Export Controls*, https://www.trade.gov/country-commercial-guides/china-us-export-controls; Jacob Kastrenakes, *Trump Signs Bill Banning Government Use of Huawei and ZTE Tech*, THE VERGE (Aug. 13, 2018), https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump; Blair Wang, *CFIUS Ramps up Oversight of China Deals in the US*, THE DIPLOMAT (Sept. 14, 2021), https://thediplomat.com/2021/09/cfius-ramps-up-oversight-of-china-deals-in-the-us/; Jones Day, *Chinese States Investments and the Committee on Foreign Investment in the United, Insights* (Jan. 11, 2018), https://www.jonesday.com/en/insights/2018/01/chinese-investments-and-the-committee-on-foreign-i.

relating to other countries and military arms export controls.[6] Section 1237 was added to the NDAA in 1998 following political pressure on then-President Clinton by the Republican Party-led Congress to monitor and restrict Chinese military expansion. However, as noted below, neither Clinton nor any subsequent U.S. president exercised their powers under this provision until over 20 years later, under President Trump.[7]

Section 1237 allows the U.S. Department of Defense, with input from the FBI, CIA, and Attorney General, to designate certain Chinese entities as CCMCs and to exercise International Emergency Economic Powers Authority ("IEEPA") against them.[8] What this means in practice is that after the U.S. President makes an executive order stating that there is a "national emergency," all U.S. persons are forbidden from purchasing or otherwise possessing the publicly traded securities of CCMCs or any derivatives of those securities.[9]

CCMCs are defined in s.1237 as any person who "is owned or controlled by, or affiliated with, the People's Liberation Army or a ministry of the government of the People's Republic of China or that is owned or controlled by an entity affiliated with the defense industrial base of the People's Republic of China." The statute further defines the People's Liberation Army ("PLA") as "the land, naval, and air military services, the police, and the intelligence services of the Communist Government of the People's Republic of China, and any member of any such service or of such police."[10]

Although this legislation was passed in 1998, and the list of CCMCs was supposed to be produced within 90 days and updated regularly, the first list was not published until June 2020. It is not clear why this lengthy delay occurred, and as Judge Contreras of the U.S. District Court of Columbia noted when hearing the applications by Xiaomi and Luokung, "this lack of use … undermines the notion that the CCMC designation process is critical to maintaining this nation's security."[11] However, since 2020, the list has been revised and expanded at least four times, and executive orders relating to CCMCs have been issued by both President Trump and President Biden, leading to a confusing legislative/executive melange that this paper attempts to decipher below.

---

[6] Effective from 1999: National Defense Authorization Act for Fiscal Year 1999, Pub. L. 105-261, 112 Stat. 2160 (Oct. 17, 1998) (as amended, hereafter "NDAA") See especially Titles XII-XV.

[7] For the history of s.1237, see Jordan Brunner, *Communist Chinese Military Companies and Section 1237: A Primer,* LAWFARE (Mar. 22, 2021), https://www.lawfareblog.com/communist-chinese-military-companies-and-section-1237-primer.

[8] *See* NDAA, s.1237(a)(b).

[9] For the President's emergency powers, see 50 U.S.C § 1701, and for the power to prohibit purchase of securities, see 50 U.S.C § 1702(a)(1): "Presidential Authorities: the President may, under such regulations as he may prescribe, … (A) investigate, regulate, or prohibit … (iii) the importing or exporting of currency or securities, by any person, or with respect to any property, subject to the jurisdiction of the United States."

[10] NDAA s.1237(b)(4)(B)(i) and s. 1237(c).

[11] *Xiaomi Corporation, et al., v. Department of Defense, et al.*, U.S. Dist. Ct. of Colum., Civ. Action No.: 21-280 (RC), 12 March 2021 (hereafter *Xiaomi*) at p. 25; and *Luokung Technology Corp. et. al., v. Department of Defense, et al.*, Civ. Action No.: 21-583 (RC), 5 May 2021 (hereafter *Luokung*) at p. 30.

The initial reason for this sudden flurry of activity was a 2019 bipartisan letter from four Senators and Congressmen. The letter claimed that there was an imminent "threat" to U.S. national security from China and reminded the Secretary of Defense that the power to designate CCMCs had never been exercised.[12] The letter also referred to China's alleged "Military-Civilian Fusion":[13]

> The CCP has adopted a strategy of "Military-Civilian Fusion" to achieve its national objectives, enlisting Chinese corporations and universities to harness emerging civilian technologies for military purposes. If Beijing cannot develop technology on its own, it attempts to steal it from the United States using cyber espionage, intelligence assets operating in the United States, and state-directed companies that acquire American firms to transfer proprietary information. As Assistant Secretary for International Security and Nonproliferation Christopher Ford has stated, Military-Civilian Fusion is the "CCP's blueprint for China's global 'return' to military preeminence."

This reference to the vague concept of Military-Civilian Fusion is crucial because it has led the CCMC list to include several Chinese corporations that have no clear military links, but are alleged by the Department of Defense to have the potential to contribute to China's military modernization and expansion. We will return to this point in a later section of this paper.

After the Department of Defense had prepared its initial list of CCMCs, then-President Trump issued Executive Order No. 13959, Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies, (Nov. 12, 2020) ("E.O. 13959").[14] President Trump declared a national emergency under IEEPA due to the "security threat" posed by "civilian Chinese companies" that support the People's Republic of China's ("PRC") military and intelligence activities. The order alleges that through a "national strategy of Military-Civil Fusions," the PRC compels civilian Chinese companies to support its military and intelligence activities, and these companies in turn "raise capital by selling securities to United States investors . . . exploit[ing] United States investors to finance the development and modernization of [the PRC's] military." President Trump concluded that these actions "allow the PRC to directly threaten the United States homeland and United States forces overseas, including by developing and deploying weapons of mass destruction, advanced conventional weapons, and malicious cyber-enabled actions against the United States and its people."[15]

---

[12] Press Release, *Cotton, Schumer, Gallagher, Gallego Urge Nod to Name Chinese Defense Companies in U.S.* (Sept. 12, 2019), https://www.cotton.senate.gov/news/press-releases/cotton-schumer-gallagher-gallego-urge-dod-to-name-chinese-defense-companies-in-us.

[13] *Id.*

[14] Executive Order No. 13959, 85 F.R. 73185 (Nov. 12, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-securities-investments-finance-communist-chinese-military-companies/.

[15] E.O. 13959.

E.O. 13959 prohibited all United States persons from engaging in select investment activities with any CCMC, including a blanket prohibition on any "transaction in publicly traded securities, or any securities that are derivative of, or are designated to provide investment exposure to such securities of any [CCMC]."[16] In January 2021, the order was updated and now expressly requires all United States persons to fully divest of any securities of a CCMC within 365 days of a company's designation as a CCMC.[17]

Following these orders and a further expansion of the list on 14th January, 2021, there were 44 Chinese firms designated as CCMCs. Three of these firms challenged their designations, seeking injunctions in the U.S. District Court (Columbia District). Two were successful – Xiaomi Corporation and Luokung Technology Corp. A detailed analysis will be provided in the following section. The third, GOWIN Semiconductor Corp., filed suit in May 2021, but it was removed from the Biden administration's updated list of sanctioned companies in June 2021 and subsequently the lawsuit was dropped.[18]

The Biden administration added some new firms and removed others, making a current total of 59 Chinese firms. Part of the reason for these revisions is that President Biden rescinded President Trump's previous executive orders and issued a new executive order (E.O. 14032) which effectively changed the definition of a CCMC.[19] The key change is the addition of a whole new category of persons/entities who operate in "the surveillance technology sector of the economy of the PRC."[20] This clearly expands the types of Chinese firms that can be sanctioned well beyond the military and defense sectors to include firms like Hikvision that produce security cameras widely used in Chinese cities for crime control and domestic surveillance by the Chinese police. We will discuss the altered definition in greater detail in a later section of this paper.

Evidently, the Biden administration is attempting to restrict U.S. investors from financing industry sectors that are perceived to be assisting the Chinese government in actions that may impact Chinese citizens within China's national territory. Nevertheless, it is not clear how this may be related to U.S. national

[16] E.O. 13959 § 1(a).

[17] Exec. Order No. 13974, *Amending Executive Order 13959—Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies*, WHITE HOUSE (Jan. 13, 2021), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-amending-executive-order-13959-addressing-threat-securities-investments-finance-communist-chinese-military-companies/.

[18] For the June 2021 list of CCMCs, see the *Annex to Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*, (Jun. 3, 2021), WHITE HOUSE ("E.O. 14032"), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/. *See also* Karen Freifeld, *Nasdaq Withdraws Listing Ban On Luokung After U.S. Judge's Decisio*n (May 6, 2021), REUTERS, https://www.reuters.com/technology/us-listing-ban-luokung-lifted-after-judges-decision-2021-05-06/.

[19] *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China (E.O. 14032)*, WHITE HOUSE (Jun. 24, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.

[20] E.O. 14032, s.1(a).

security and why firms in these sectors are a threat to U.S. citizens. The executive order tries to circumvent the criteria of military links or national security threats by removing references to the NDAA altogether, and referring to the relevant firms as "certain companies of the People's Republic of China," instead of the loaded term "Communist Chinese military companies." However, the emergency powers authority underpinning this executive order still requires evidence of an "unusual and extraordinary threat … to the national security, foreign policy, and economy of the United States," and it is not clear that it would survive a court challenge by a civilian Chinese firm.[21]

Beyond the legal technicalities, the continued arbitrary nature of these economic sanctions under the Biden administration will likely fail to convince either the Chinese leadership or other outside observers that the U.S. government respects the rule of law, thus failing to attain their stated goals.

To support these assertions, we will first analyze two U.S. court decisions where Chinese companies successfully challenged their designation as CCMCs. These decisions clearly demonstrate the arbitrary process by which U.S. government regulators selected companies for sanctions and the lack of any principled national security basis for placing certain Chinese companies on the CCMC list.

III. TESTING THE EVIDENCE IN COURT: THE XIAOMI AND LUOKUNG CASES

While the definition of CCMCs has changed since these court decisions were issued, the basic principles of due process and concerns about the overreach of executive powers remain highly relevant to the current sanctions list. Particularly disturbing is the failure of the Department of Defense to engage in any careful research on these two Chinese firms' businesses before wrongly designating them as CCMCs, not to mention the significant financial and reputational harm caused to the companies.

Both the Xiaomi and Luokung cases were heard by Judge Rudolph Contreras of the District of Columbia Court – in March and May 2021 respectively – and the arguments and reasoning in the two decisions are very similar. The court found that both companies had shown a high chance of winning their challenge to the Department of Defense's ("DoD") actions and they would suffer irreparable harm if a preliminary injunction to remove them from the list of CCMCs was not approved.

The companies challenged the DoD on the ground that government officials had acted in an "arbitrary and capricious" manner, which breached the Administrative Procedure Act ("APA").[22] The court accepted this argument

[21] E.O. 14032, preamble, and cf. 50 U.S. Code § 1701: Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities.

[22] The plaintiffs also raised a constitutional challenge, arguing that the DoD's actions deprived them of a property and liberty interest under the Fifth Amendment: see *Xiaomi*, at 6, 16 n.8; *Luokung*, at 8, 24 n.13. The court found it unnecessary to decide the constitutional issue, but noted that this argument also "raised serious concerns."

for several reasons. First, despite the greater deference that courts must show to government actions involving national security, there is still a need for the government to "articulate a satisfactory explanation for its actions"; second, it must show a "rational connection" between its actions and the relevant legislation; and finally, it must demonstrate that its conclusions are supported by "substantial evidence."[23]

The DoD failed on all these grounds. The court found that its brief memoranda justifying placing Xiaomi and Luokung on the CCMC list did not even refer to the relevant legislation (NDAA s.1237), and there was "no rational connection" between the facts listed about the companies and the definition of a CCMC in the legislation.[24]

For Xiaomi, which primarily manufactures and sells mobile phones to consumers, the DoD merely drew a couple of statements from the company's 2019 annual report noting that Xiaomi was investing heavily in 5G and artificial intelligence (AI), two types of technology the DoD claimed are "essential to modern military operations," and that Lei Jun, Xiaomi's founder and CEO, was awarded the title of "Outstanding Builder of Socialism with Chinese Characteristics" by the Chinese Ministry of Industry and Information Technology. The court dismissed both these claims, noting that as a consumer electronics firm, Xiaomi had to keep up with recent technological changes in its industry sector and to assume without further evidence that every company involved in 5G and AI is a CCMC would be an over-reach of government power:[25]

That 5G and AI technologies have military applications as well cannot be enough to support the conclusion that Xiaomi is a CCMC. Indeed, such an outcome could result in a situation where any Chinese company involved in technology that has alternative military uses could be designated as a CCMC. Moreover, it would appear that even U.S. technology companies with Chinese subsidiaries could be considered CCMCs under this sweeping inference. Needless to say, the Court is troubled by the lack of any limiting principle on the Department of Defense's CCMC designation power if this logic is allowed to stand.

On the issue of Lei Jun's achievement award from a Chinese government ministry, the court found that Chinese entrepreneurs in many different civilian industries received the same award, and there was no evidence that it was due to Xiaomi being involved in the Chinese "civil-military fusion."[26]

Similarly, in the case of *Luokung*, the DoD's claim was also based on information pulled from Luokung's website and general media articles, including: that the company designs technology with "potential" military/police and space program applications, such as AI and autonomous

[23] *Xiaomi*, at 7–8; *Luokung*, at 9–11.
[24] *Xiaomi*, at 9–10; *Luokung*, at 10–11.
[25] *Xiaomi Corporation v. Department of Defense*, No. 21-280 (RC), at 14–15 (D.D.C. Mar. 12, 2021).
[26] *See id.* at 16.

systems; and that it had announced agreements with Chinese government entities, SOEs, and other alleged CCMCs like Huawei Technologies, to "promote the wide application of geospatial information data and technical services in spatial planning, e-government, smart city, smart ecology, and smart agriculture."[27] However, as with Xiaomi, the court found that Luokung's products were for civilian use, that the DoD had not provided any evidence of the company's affiliation with the military or Chinese police, and that "at most, the facts allow the conclusion that Luokung may currently or will one day provide products to entities with ties to the Chinese state. This behavior is no different than American technology companies such as Apple. This is simply not enough to demonstrate it is under the 'effective control' of the Chinese state or military."[28]

In both cases, the court found that the companies would suffer irreparable harm by being de-listed from U.S. securities markets, thereby being excluded from access to essential finance, and they would lose a significant number of U.S. and international investors, key customers, and executive talent due to their designation as CCMCs. Their international reputation would also suffer due to being incorrectly branded, in the words of the executive order, as companies that "directly support the PRC's military, intelligence, and security apparatuses" and "allow the PRC to directly threaten the United States homeland and United States forces overseas."[29]

Finally, the court found that the public interest would not be served in allowing the government's actions to stand, as it had not shown that any "weighty national security concerns" were at stake in relation to the two companies. By contrast, there was a "substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations."[30]

This was a decisive rejection of the arbitrary process by which these two companies had been included on the list of CCMCs. A key point here was the court's interpretation of the definition of CCMCs in s.1237 of the NDAA, namely the phrase "owned or controlled by, or affiliated with, the People's Liberation Army or a ministry of the government of the People's Republic of China or that is owned or controlled by an entity affiliated with the defense industrial base of the People's Republic of China." It was clear that neither Xiaomi nor Luokung met the "owned or controlled by" test, as both are publicly traded firms in the U.S. with widely held shares, and their largest shareholders are Chinese individuals with no military or government positions. The DoD's argument relied on a dictionary definition of "affiliate", that a company would

[27] *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 19–20.

[28] *See id.* at 20–22.

[29] *Xiaomi Corporation v. Department of Defense*, No. 21-280 (RC), at 17-24 (D.D.C. Mar. 12, 2021); *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 25–30.

[30] *Xiaomi Corporation v. Department of Defense,* No. 21-280 (RC), at 24–25 (D.D.C. Mar. 12, 2021); *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 30–32.

be "affiliated with" the Chinese government, the PLA, or the defense industrial base of the PRC, should the company have a "common purpose" or "shared characteristics" with the PRC government/military/police, or be "closely associated in a dependent or subordinate position."[31]

The court dismissed this very broad definition in favour of a standard legal definition of "affiliate" that appears in several U.S. statutes, including the DoD's own regulations. This legal definition has been widely followed by federal courts, namely: "An 'affiliate' is 'any person that controls, is controlled by, or is under common control with another person'" … and "an 'affiliate' is an 'entity that directly or indirectly controls, is directly or indirectly controlled by, or is under common control with, the ultimate parent entity.'"[32] The court's concern was that the DoD's definition would contradict the clear wording of statutes and would allow the U.S. executive branch "almost no limiting principle." It would potentially include any company that signed a contract with a Chinese government entity, regardless of the existence of any connection with military or police applications.[33]

IV. BIDEN ADMINISTRATION'S RESPONSE AND CRITICAL ANALYSIS OF COMPANIES ON THE BIDEN LIST

While Xiaomi and Luokung have been removed from the latest U.S. government list following litigation, in its latest executive order, the Biden administration has attempted to sidestep the definition problem by removing references to CCMCs and NDAA s.1237 altogether. The order (E.O. 14032) includes an Annex of 59 Chinese firms, effectively expanding on the previous list. Instead of the term "Communist Chinese military company," the order adopts a much vaguer designation of "Certain Companies of the People's Republic of China." It then defines the companies to be included on the list as follows:[34]

> … any person determined by the Secretary of the Treasury, in consultation with the Secretary of State, and, as the Secretary of the Treasury deems appropriate, the Secretary of Defense:
>
> (i) to operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of the PRC; or
>
> (ii) to own or control, or to be owned or controlled by, directly or indirectly, a person who operates or has operated in any sector described in subsection (a)(i) of this section, or a person who is listed in the Annex to this order or who has otherwise been determined to be subject to the prohibitions in subsection (a) of this section.

[31] *Xiaomi Corporation v. Department of Defense,* No. 21-280 (RC), at 11–12 (D.D.C. Mar. 12, 2021); *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 12–13.

[32] *Xiaomi Corporation v. Department of Defense,* No. 21-280 (RC), at 12–13 (D.D.C. Mar. 12, 2021); *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 13–17.

[33] Xiaomi Corporation v. Department of Defense, No. 21-280 (RC), at 13 (D.D.C. Mar. 12, 2021); *Luokung Technology Corp. et. al., v. Department of Defense, et al,* at 18.

[34] E.O. 14032, s.1(a).

Apart from moving the power to designate companies from the DoD to the Treasury Department, the main differences are: first, the definition no longer uses the term "affiliated with" which was found to be too broad in the Xiaomi and Luokung cases, making ownership and direct/indirect control the only remaining test. Second, the definition no longer includes entities controlled by or affiliated with a "ministry of the People's Republic of China," which would potentially capture all Chinese state-owned enterprises and prevent any foreign investment in those firms. Third, the definition makes no reference at all to "Communist Chinese military companies" or the definition of CCMCs in NDAA s.1237, and instead uses the phrase "operate or have operated in the defense and related materiel sector." Finally, it makes explicit what was only implicit in the previous definition: not only military-defense firms but also any civilian firms operating in the "surveillance technology sector of the economy of the PRC" may be included on the list.

An initial list of 59 companies is annexed to the executive order, but it gives power to the Treasury Secretary to add and remove companies from the list.[35] The consequences of being placed on the list remain the same, namely, a prohibition on U.S. persons purchasing or selling those companies' publicly traded securities.[36]

Will this altered definition protect the Treasury Department from challenges by companies that are placed on the list? Based on the cases of Xiaomi and Luokung, to justify its actions in the face of a lawsuit, the government will still need to "articulate a satisfactory explanation for its actions," to show a "rational connection" between its actions and the relevant executive order, and that its conclusions are supported by "substantial evidence." In other words, as Judge Contreras put it in the *Luokung* case, there is still a public interest in "having governmental agencies abide by the federal laws that govern their existence and operations."[37] Based on our analysis in the following section, the list includes a wide range of firms in many different industries, and the connection with either the "defense/materiel sector" or the "surveillance technology sector" in several cases appears to be tenuous at best.

A. Biden's List Compared to Trump's Lists

At first sight, Biden's list looks quite different from that of Trump. Rather than five separate "tranches" totaling 44 companies, Biden's executive order includes a single list of 59 companies. The Whitehouse "Fact Sheet" that accompanied the executive order further divides Biden's list into three sections: Group 1 companies are in the "*Defense and Related Materiel Sector*" (50 firms); Group 2 companies in the "*Surveillance Technology Sector*" (2 firms);

[35] For removal powers, see E.O. 14032, s.6. For the previous definition, see NDAA s.1237(b)(4)(B)(i) and s. 1237(c), and NDAA, s.1237(a)(b).

[36] E.O. 14032, s.1(a).

[37] *Luokung*, at 30–32; and cf. *Xiaomi*, at 24–25. *Luokung* pp. 30-32; and *Cf. Xiaomi Corporation v. Department of Defense* p. 24–25.

and Group 3 companies are those who "*Own or Control, or Are Owned or Controlled by, Directly or Indirectly, a Person Who Operates or Has Operated in at Least One of These Two Sectors*" (10 firms).[38]

However, looking more closely, the two companies in Group 2, Hikvision Ltd and Huawei Technologies, also appear in Group 1; several of the companies in Group 1 are affiliated with each other in the Aviation Industry Corporation of China ("AVIC") conglomerate, whereas Trump's lists only referred to one AVIC corporation; and all of those in Group 3 are either parent or subsidiary companies of those in groups 1 and 2. So Biden's list is more like a clarification of Trump's list rather than an expansion.

In fact, fifteen corporations on the previous list have been removed from Biden's list. The three private firms that brought injunction suits against the Department of Defense are no longer there (Xiaomi, Luokung, and GOWIN Semiconductor). [39] Several state-owned enterprises that do not have any obvious military links or surveillance technology businesses have also been removed, including the Commercial Aircraft Corporation (COMAC, which builds civil aircraft), China Three Gorges Corporation (which constructs and operates hydroelectric power plants), and Beijing Zhongguancun Development Investment Center (a business-to-business platform providing IT solutions and IT services to commercial companies).[40] The removal of these companies is a tacit admission by the Biden administration that they should not have been placed on the list in the first place.

Biden's list also corrects some errors and omissions in the Trump list. For example, in tranche 5 of the former list, the name of Luokung was spelled incorrectly and remained that way for two months;[41] and in tranche 1, a company called "Huawei" was included, but this is not the full name of any

[38] Because of some overlaps between the three groups, with the two Group 2 companies appearing in Group 1 as well, and Panda Electronics Group Co. Ltd. inexplicably appearing in both Group 1 and Group 3, the total of the three groups adds up to 62 companies, but only 59 of these are discrete corporations. See White House, *Fact Sheet: Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*, THE WHITE HOUSE, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/03/fact-sheet-executive-order-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.,(last visited Jul. 10, 2023) (hereafter, "White House Fact Sheet").

[39] Luokung's listing on the NASDAQ was reinstated following its successful lawsuit, and GOWIN Semiconductor withdrew its lawsuit after it was removed from the list. Xiaomi's listing on the Hong Kong Stock Exchange was never suspended, but its shares rose 20%, presumably because U.S. institutional investors were once again permitted to purchase its shares: *see* Gowin, *GOWIN Removed from CCMC List, Withdrawing Lawsuit*, GOWIN., https://www.gowinsemi.com/en/about/detail/latest_news/70/ (last visited Jul. 10, 2023); Karen Freifeld, *UPDATE 1-Nasdaq Withdraws Listing Ban on Luokung after U.S. Judge's Decision*, REUTERS, https://www.reuters.com/article/usa-china-luokung-tech-idCNL1N2MT26H,, (last visited Jul. 10, 2023); Siladitya Ray, *Pentagon Agrees To Remove Chinese Smartphone Giant Xiaomi From Trump-Era Blacklist*, FORBES, https://www.forbes.com/sites/siladityaray/2021/05/12/pentagon-agrees-to-remove-chinese-smartphone-giant-xiaomi-from-trump-era-blacklist/?sh=3ae0c4e548c4 (last visited Jul. 10, 2023).

[40] For the full list of fifteen removed corporations, see Jordan Brunner and Emily Weinstein, *The Strategic and Legal Implications of Biden's New China Sanctions*, LAWFARE, https://www.lawfareblog.com/strategic-and-legal-implications-bidens-new-china-sanctions (last visited Jul. 10, 2023).

[41] Noted by the judge in *Luokung Technology Corp. et. al., v. Department of Defense, et al.*, at 5–6.

specific Huawei corporation (of which there are dozens throughout the world). By contrast, Biden's list gives the full English name of Huawei Technologies Co., Ltd. which controls Huawei's Chinese and global operations, as well as its parent corporation Huawei Investment & Holding Co., Ltd., through which Huawei's shares are held by its employee shareholding fund. Biden's list also adds two of Huawei's investment corporations that it uses to raise funds through bond issues, Proven Glory Capital Limited and Proven Honour Capital Limited.[42]

Likewise, the parent corporations of China Mobile, China Telecom, and China Unicom were included on Trump's list, but their partially owned subsidiary corporations that are listed on stock exchanges in either the U.S. or Hong Kong/Shanghai were omitted. This obviously led to confusion about whether U.S. investors could continue to buy shares in those separate corporations, even causing the New York Stock Exchange to reverse its initial de-listing of these subsidiaries. Biden's list added the relevant subsidiary corporations to offer some clarity, and these subsidiaries were removed from trading on the NYSE in May 2021.[43] These kinds of careless omissions that once caused unnecessary confusion are further evidence of the undue haste and failure to conduct basic research when the initial lists were compiled by the Department of Defense.[44]

At first sight, Biden's list appears to be more carefully prepared and less arbitrary in its selection of companies than the five tranches issued during Trump's presidency. However, a deeper review of the remaining companies on the list suggests otherwise.

B. Critical Examination of Biden's List

The original aim of the "Communist Chinese military companies" lists was to prevent United States individuals and entities from supporting China's military activities through their capital investments. This aim may be justifiable from the U.S. perspective given the potential instability in the East Asian region as a result of a rising China, not to mention its ongoing disputes with U.S. ally regions and states (Taiwan, Japan, South Korea and the Philippines), and territorial issues relating to islands and reefs in the South China Sea. These risk factors have in part led to increases in both the US and Chinese defense budgets, which together accounted for almost two-thirds of the total increase in global

[42] We discuss Huawei in more detail below..

[43] Contrast in between the two NYSE's announcements: Christine Wang, *NYSE Says It Will No Longer Delist Three Chinese Telecom Giants*, CNBC Markets, *available at* https://www.cnbc.com/2021/01/05/nyse-says-it-will-no-longer-delist-three-chinese-telecom-giants.html (Jan. 4, 2021), ; Reuters, *Three Chinese Telecom Companies To Be Delisted by NYSE*, REUTERS, *available at* https://www.reuters.com/business/media-telecom/three-chinese-telecom-companies-be-delisted-by-nyse-2021-05-07/ (May 8, 2021).

[44] Neither Trump's nor Biden's lists include the Chinese names of any corporations, which would have helped to clear up some of this confusion.

defense spending in 2020, though clearly US spending still greatly exceeds that of China.[45]

However, the Biden administration (like its predecessors) has confused its aim by mingling together Chinese military defense firms with civilian firms that have no clear military focus. Part of this confusion may lie in the complex history of some Chinese technology firms that were originally part of the defense sector but subsequently became civilian commercial firms. The make-up of the current ecosystem of Chinese defense SOEs started in the late 1990s. Then-President Jiang Zemin reformed the outdated and inefficient centrally planned state military factories set up during the Cultural Revolution, many of which were in inaccessibly remote locations.[46] In particular, the 15th Chinese Communist Party (CCP) Congress in 1997 launched a major restructuring of the defense industry in five core sectors: aviation, space, nuclear, shipbuilding, and land warfare.[47] In the following decades, numerous SOEs were reconsolidated, restructured, or merged, with new SOEs incorporated.[48] The objective was to increase competition and transform these entities into more efficient corporate organizations, thereby upgrading their technologies and improving the performance of their military products to meet what the Chinese government viewed as threats from "hostile foreign powers" in the 21st century.[49]

At the same time, the military was required to divest its ownership and control of thousands of commercial businesses that served no military function but were used to funnel money into the military when government funding was limited.[50] The involvement of the military in civilian businesses led to corruption and abuse of power, including bribery of public officers to turn a blind eye to smuggling, illegal drug dealing, and other organized criminal activity.[51] The most notorious example was the corporate empire of Lai Changxing, a private entrepreneur who bribed local military corporations and police officials in Fujian Province during the 90s to smuggle automobiles,

[45] International Institute for Strategic Studies, *The Military Balance 2021*, vol. 121 (Taylor & Francis 2021), pp. 517–22, (accessed March 30, 2023) .

[46] For the Maoist period military/civilian factories located on the so-called "third front" in the Chinese hinterland, see COVELL F. MEYSKENS, MAO'S THIRD FRONT: THE MILITARIZATION OF COLD WAR CHINA (2020); and Barry Naughton, *The Third Front: Defense Industrialization in the Chinese Interior*, 115 CHINA Q. 351–386 (1988).

[47] *See* EVAN S. MEDEIROS, ROGER CLIFF, KEITH CRANE & JAMES C. MULVENON, A NEW DIRECTION FOR CHINA'S DEFENSE INDUSTRY, ch. 1 (2005); *see also* RICHARD A. BITZINGER, ARMING ASIA: TECHNONATIONALISM AND ITS IMPACT ON LOCAL DEFENSE INDUSTRIES (2016).

[48] Lucie Béraud-Sudreau & Meia Nouwens, *Weighing Giants: Taking Stock of the Expansion of China's Defense Industry*, 32 (2) DEF. & PEACE ECON. 151–77 (2021).

[49] *Supra* note 47.

[50] *See* James Mulvenon, *Soldiers of Fortune: The Rise and Fall of the Chinese-military Business Complex*, 1978-1998, at 99–101, 186–189 (2001), https://www.bicc.de/uploads/tx_bicctools/paper15.pdf.

[51] The corruption continued into the 2000s: James Mulvenon, *To Get Rich Is Unprofessional: Chinese Military Corruption in the Jiang Era*, 6 CHINA LEADERSHIP MONITOR 21, 21–35 (2003).

natural resources, and other products, altogether amounting to billions of dollars worth, while evading customs duties.[52]

Since the late 1990s, the CCP has steadily sought to modernize its military and transform the defense industries into more focused organizations. By massively increasing military funding, the CCP wanted its military to stop engaging in corrupt business activities that weakened the party's authority and distracted the armed forces from their duty to defend the nation.[53] Defense SOEs have emerged from this ongoing restructuring and operate on a massive scale. These companies make no secret of their direct involvement in supplying weaponry or technology to the Chinese military. It is therefore relatively easy to classify Chinese companies in aviation, space, nuclear, shipbuilding, and land warfare sectors as "defense or related materiel" firms, based on a brief review of their websites, as noted below.

However, following the divestments since the late 1990s, some former military companies have become exclusively civilian in their operation. There is no justification in assuming that they still maintain hidden links to the military, as we analyze further below. Secondly, it is true that many Chinese companies supply civilian consumer products they produce to military customers. But this does not make these companies a part of what Western commentators have called a "military-civil fusion" (MCF) in which the so-called civilian companies (including many privately-owned firms) are allegedly assisting the Chinese military in developing weaponry and technology. Without further evidence, it also fails to justify treating such firms as "military companies" that threaten the national security of the US and its allies.[54] Yet, in discussions of the MCF, the boundary between a firm that actively supports the military with defense technology and one where the military just happens to purchase civilian products or services as a customer is blurred, causing the kind of confusion that was apparent in the Xiaomi and Luokung cases.[55]

A further complication arises with the addition of a whole new category of non-military "surveillance technology" companies, as it muddies the original focus of the CCMC list – the alleged national security threat to U.S. citizens – and broadens the list to include actions by the Chinese government on Chinese citizens within China's national territory. It is not clear how the way the Chinese government is treating Chinese citizens poses a threat to U.S. citizens,

[52] Shawn Shieh, *The Rise of Collective Corruption in China: The Xiamen Smuggling Case*, 14 (2) J. CONTEMP. CHINA 67–91 (2005); and for an excellent narrative account, see OLIVER AUGUST, INSIDE THE RED MANSION: ON THE TRAIL OF CHINA'S MOST WANTED MAN (2007).

[53] *Supra* note 47; and IISS, *The Military Balance*, at 228–35.

[54] For US government assertions, see the preamble to E.O. 13959. For a more balanced account comparing US and Chinese approaches, see Elsa B. Kania, *In Military-Civil Fusion, China Is Learning Lessons from the United States and Starting to Innovate*, The Strategy Bridge (Aug. 27, 2019), https://thestrategybridge.org/the-bridge/2019/8/27/in-military-civil-fusion-china-is-learning-lessons-from-the-united-states-and-starting-to-innovate.

[55] *Xiaomi*, *supra* note 11, at 14–15 (comments of Judge Contreras); and *Luokung*, *supra* note 11, at 20–22.

providing no ground for such an "emergency" executive order. It is difficult to identify any "rational connection" between those actions and an executive order focusing on the national security threat to the U.S.[56]

These complications reflect an unresolved debate within U.S. policy circles (and those of other liberal democracies) as to whether the scope of economic sanctions should be limited to demonstrably hostile Chinese entities, such as overt military/defense firms, or whether it should be broadened to include virtually any Chinese commercial entity that has supplied products which have been used, or potentially may be used, by the military or police/security forces/CCP.[57] Together, they raise the thorny question as to whether sanctions and punishment or trade and cooperation are the best way to resolve contradictions in U.S.-China relations. We will respond to this question in the Conclusion.

1. Corporations with Clear Defense or Related Materiel Businesses. To investigate the companies on Biden's list, this paper relies on a broad range of publicly available information. Chinese defense companies and their subsidiaries are generally eager to present themselves as suppliers of the PLA or other armed forces, as this is a source of national pride. The idea commonly suggested by Western commentators that large Chinese companies would generally conceal their links to the military or the Chinese government is unfounded.[58] Company websites are a useful source of information, along with relevant information published by the Stock Exchanges where many of the corporations are listed.

In situations where company sources do not provide clear or sufficient evidence, we also look at a range of Chinese and English-language media sites, reports by research think tanks, reports from U.S. and other government investigations, available published accounts of company histories, and registered Chinese shareholding databases. These sources can be useful to verify if a civilian Chinese company has supplied products and services to the military or engaged in other activities that may pose a threat to U.S. national security. However, as we discuss further below, some of these sources are

[56] For the "rational connection" test of government action, see *Xiaomi*, *supra* note 11, at 7–8; and *Luokung*, *supra* note 11, at 9–11.

[57] Donald Trump's former trade advisor, Peter Navarro, is typical of the China "hawks" who see any co-operation with China as a threat to the US: *see* PETER NAVARRO, CROUCHING TIGER: WHAT CHINA'S MILITARISM MEANS FOR THE WORLD (2015); a counterargument emphasizing the drawbacks of economic decoupling can be found in US CHAMBER OF COMMERCE AND RHODIUM GROUP, UNDERSTANDING DECOUPLING: MACRO TRENDS AND INDUSTRY IMPACTS (2021). And for two contrasting views from Australia, see PETER HARTCHER, RED ZONE: CHINA'S CHALLENGE AND AUSTRALIA'S FUTURE (2021), and GEOFF RABY, CHINA'S GRAND STRATEGY AND AUSTRALIA'S FUTURE IN THE NEW GLOBAL ORDER (2020).

[58] For Chinese firms' willingness to disclose their military links, see the Appendix, *infra* at 39–47, for the public websites of Chinese defense sector corporations. For U.S. claims about concealment of military links, see the discussion of Huawei Technologies below, especially the PSC Report cited there. For a more balanced discussion of Chinese civil-military fusion, see Kania, *supra* note 54.

speculative and biased, relying on unproven inferences and exaggeration, so they must be used with caution.

It may be that in selecting Chinese corporations for sanctions, the Department of Defense relied on classified information that clearly justified its decisions. Unfortunately, we have no access to such information, which may be a weakness of this study. However, we have reasons to believe that this is not the case for the vast majority of corporations on the list, because when challenged by lawsuits, the lawyers for the Department of Defense made no reference to any classified information, and did not even suggest to the judge that their decision was even partially based on intelligence reports.[59] It appears, therefore, that the legality of placing any corporation on the list will stand or fall based on publicly available information about the corporation rather than classified intelligence, if any exists.[60]

Based on the available information, the majority of companies on Biden's list do have obvious military backgrounds, producing weaponry, military vessels, defense technology, fighter jets, and so on, for the Chinese military. Of the 50 "*Defense and Related Materiel Sector*" companies in Group 1, 41 of them can be easily confirmed as defense companies or companies with clear military connections. See the full list of such firms in the Appendix, Table 1, where for clarity we have placed each firm in its relevant industry sector.

2. Corporations Without Clear "Defense or Related Materiel" Businesses. Though it is clear that the 41 corporations listed in Appendix Table 1 are in the "defense or related materiel" sectors, there remain 9 companies whose military defense links are not at all clear from public materials. We list these firms in the Appendix, Table 2, and then divide them into industry sectors for more detailed analysis below. The sectors include infrastructure/resources, telecommunications, semiconductors, and electronics/information technology.

a. Infrastructure and Resource Firms. The first three corporate groups in Table 2 are all state-owned enterprises (SOEs) controlled by the central government, but there is no indication that they are involved in "defense or related materiel" sectors.

China Railway Construction Corporation Limited (CRCC) is one of the largest construction and engineering conglomerates in the world. CRCC is listed on the Shanghai and Hongkong Stock Exchanges with a State ownership of 51.13% via its parent company China Railway Construction Group Co. Ltd. as of the end of 2020. The remaining shares are held by members of the public

[59] For the two lawsuits that have been heard by courts, the DoD's lawyers relied totally on information published by the companies themselves, plus some publicly available media reports. See *Xiaomi* and *Luokung* decisions discussed above.

[60] See also the discussion of Huawei Technologies below, where intelligence officials privately admitted to reporters from the *Los Angeles Times* that they did not have incriminating information about the company's alleged links to the military.

or institutional investors, purchased in Shanghai (33.58%) or Hong Kong (15.29%).[61]

The main business activities of CRCC include the following:

Contract construction projects e.g. airports, railways, tunnels, and highways;

Land survey and design consultation, e.g. designing the subway network in Suzhou City; the Zhejiang Provincial railway PPP project; a river diversion project in Shandong Province, etc.;

Real estate construction projects. By the end of 2020, CRCC had completed 328 residential construction projects across 77 cities in China;

Construction equipment manufacture. CRCC is the largest manufacturer in China of construction equipment, specializing in large-scale machinery and equipment such as road maintenance machinery, tunneling machinery, and lifting equipment;

Logistical services, such as iron ore and concrete procurement, and manufacturing, transport, and supply of building materials;

Financial services including loans, risk consulting, insurance, and deposits;

Emerging industrial construction services, such as large-scale prefabricated construction industrial parks, solar farms, and wind power projects.

Our research shows that CRCC is a large SOE operating on a massive scale in multiple fields and numerous countries. CRCC has certainly completed many important State-funded infrastructure projects including high-speed railways and airports, but there is no information suggesting CRCC's connection to the military.

It is true that a review of the company's history shows that CRCC originated from the Chinese People's Liberation Army (PLA) Railway Soldiers (RS) in 1948. In other words, it used to be a branch of the defense force whose role was to protect China's railways from attack, while also expanding the railway system through construction.[62] However, in 1984, the RS division was separated from the defense force, and its employees were demobilized. The Railway Ministry was then set up to take over all businesses and operations from RS. In 1990, China Railway Construction Corporation was established, signaling the new era of the corporatization of state enterprises' business functions in this sector. CRCC has been operating as an autonomous company since, though still majority shareholder-owned by the central government

[61] For the company's share structure, see *2020 Niandu Baogao* (2020 年度报告) [*2020 Annual Report, China Railway Construction Corporation Limited*], https://www.crcc.cn/col/col173/index.html. For its business operations, see also *Qiye Jianjie* (企业简介) [*Enterprise Profile,* China Railway Construction Corporation Limited *(2022)*], https://www.crcc.cn/col/col1569/index.html, and *Business*, China Railway Construction Corporation Limited (2021), China Railway Construction Corporation Limited Project Contracting (crcc.cn).

[62] *Gongsi Jianjie* (公司简介) [*Company Introduction, China Railway Construction Corporation Limited (2021)*], https://www.crcc.cn/col/col1569/index.html; and for more detail on the Railway Soldiers and other early PLA construction divisions, see Thomas J. Bickford, *The People's Liberation Army and Its Changing Economic Roles: Implications for Civil-Military Relations*, *in* CHINESE CIVIL-MILITARY RELATIONS: THE TRANSFORMATION OF THE PEOPLE'S LIBERATION ARMY, (Nan Li ed., 2006); and DANGDAI ZHONGGUO CONGSHU BIANJI BU (《当代中国》丛书编辑部), DANGDAI ZHONGGUO JUNDUI QUNZHONG GONGZUO (当代中国军队群众工作) [Contemporary China's Military Mass Work] (1988).

through its shareholding body, the State-Owned Assets Supervision and Administration Commission (SASAC).[63]

CRCC was listed on the Shanghai and Hong Kong Stock Exchanges in 2008. The financial information of CRCC shows that the vast majority of its revenues came from its residential construction projects and its B2B supply chains for construction materials.[64]

Apart from its distant origin as part of the PLA's national railway construction force, which is no longer relevant to the current corporation, there exists no other evidence suggesting CRCC's "defense or related materiel" links. There are some negative reports about the firm's overseas operations, such as alleged fraud and corruption which prevents CRCC from bidding on World Bank projects, and worker exploitation at Olympic stadium construction sites in Qatar, but while concerning, these are not defense or national security issues.[65]

China Communications Construction Company Limited (CCCCL)

Founded by its parent company China Communications Construction Group Ltd. (CCCG, which is also on Biden's list in Group 3), CCCCL principally engages in the design and construction of transportation infrastructure, dredging, and heavy machinery manufacturing. This is another centrally-controlled SOE with ultimate State ownership through SASAC which holds 57.99% of the shares. CCCCL is listed in Shanghai and Hong Kong with its minority shares widely owned by the public.[66] Similar to CRCC, it is a massive conglomerate with dozens of direct subsidiary companies and hundreds of branches/affiliated companies in a range of construction-related industry sectors.

CCCCL's main business activities include the following:[67]

> Contract construction projects, e.g. Shanghai Yangshan Deepwater Port Project; Yangtze River Estuary Deep Water Channel Regulation Project; and Jamaica North-South Highway project;

---

[63] For more discussion of SASAC and corporatization of SOEs, see Barry Naughton, *The transformation of the state sector: SASAC, the market economy, and the new national champions*, *in* STATE CAPITALISM, INSTITUTIONAL ADAPTATION, AND THE CHINESE MIRACLE ch. 3 (Barry Naughton & Kellee E. Tsai eds., 2015).

[64] *2020 Niandu Baogao* (2020 年度报告) [*2020 Annual Report, China Railway Construction Corporation Limited*], https://www.crcc.cn/col/col173/index.html.

[65] *See* RWR Advisory Group, *The U.S. Capital Markets Footprints of the Pentagon's 'First Tranche' List of PLA-Affiliated Chinese Enterprises Operating in the United States* (June. 30, 2020), https://www.rwradvisory.com/wp-content/uploads/2020/07/RWR_Pentagon_List_Report.pdf.

[66] See *Gongsi Gaikuang* (公司概况) [*Corporate Summary, China Communications Construction Company Limited (2022)*], https://www.ccccltd.cn/aboutus/gsgk_558/; *and Fazhan Licheng* (发展历程) [*Development Milestones*], https://www.ccccltd.cn/aboutus/fzlc/. For details of share ownership, see *Jiben Xinxi* (基本信息) [*Basic Information*], https://www.ccccltd.cn/tzzgx/jbxx_677/ and *2020 Niandu Baogao A Gu* (2020年度报告A股) [*2020 Annual Report, A Shares, China Communications Construction Company Limited*], https://www.ccccltd.cn/tzzgx/dqbg_682/.

[67] *Yewu Lingyu* (业务领域) [*Main Products and Services, China Communications Construction Company Limited (2022)*], https://www.ccccltd.cn/ywly/gczcb/.

Urban complex development builder and operator, e.g. Guangzhou Nansha New District Development Project, and Sri Lanka Port City project;

Major real estate developments, e.g. Greentown Hainan Blue Bay Town development project, and Nanshan Meilu development;

Infrastructure integrated investment, e.g. the Chaotianmen Bridge project, and Guiyang Dujun Highway project;

Marine heavy industry and port machinery manufacture, with key products such as quayside container cranes; 12,000-ton full-slewing crane ships; and 3000-ton offshore oil crane pipe-laying ships;

Financial services, such as supply chain investment, insurance products, and inter-bank loans.

Similar to CRCC, CCCCL operates on a huge scale and in multiple domains. The company has completed numerous major national infrastructure projects of great significance to China's development, including ports and highways. CCCCL has also established 193 branches and subsidiaries overseas in 153 countries and cities to undertake various large-scale construction projects for both foreign states and overseas private developers. According to the information on CCCCL's website, CCCCL is currently the world's largest company in the sectors of port design and construction, road and bridge design and construction, dredging, container crane manufacturing, and offshore oil-drilling platform design.[68]

According to the CCCCL's *2020 Annual Report*, the company's annual revenues exceeded RMB 627 billion (US$ 98 billion), with a net profit of RMB 16.2 billion (US$ 2.54 billion), of which the value of newly signed contracts in overseas countries and regions reached almost RMB 205 billion (approximately US$ 29.7 billion), accounting for around 19% of the newly signed contract value of the entire group. Main business activities continued to be government-contracted infrastructure construction projects, both in China and for overseas governments, including for its surveying and infrastructure-related consulting services.[69]

CCCCL has been a contractor for numerous Belt and Road Initiative projects. Although some projects may face potential corruption and environmental pollution allegations, CCCCL was recognized in the Belt and Road Top 100 Chinese Enterprises list.[70] Despite these obvious government

[68] *Gongsi Gaikuang* (公司概况) [*Corporate Summary, China Communications Construction Company Limited (2022)]*, https://www.ccccltd.cn/aboutus/gsgk_558/.

[69] *See 2020 Niandu Baogao A Gu* (2020年度报告A股) [*2020 Annual Report, A Shares, China Communications Construction Company Limited*], https://www.ccccltd.cn/tzzgx/dqbg_682/; *see* also Anon., *Zhongguo Jiao Jian 2020 Nian Shixian Jing Lirun 162 Yi Yuan* (中国交建2020年实现净利润162亿元) [*China Communications Construction Limited achieved a net profit of 16.2 billion yuan in 2020*], Zhongguo Zhengquan Bao (中国证券报) [CHINA SEC. J.] (Mar. 31, 2021), https://finance.eastmoney.com/a/202103311866855480.html.

[70] *See* Sheridan Prasso, *A Chinese Company Reshaping the World Leaves a Troubled Trail: CCCC, Belt and Road's biggest builder, is besieged by allegations of fraud, corruption, and environmental damage*, Bloomberg Businessweek, Sept. 10, 2018; Dipanjan Roy Chaudhury, *World Bank bans Chinese companies again for financial crimes*, The Economic Times, Aug. 23, 2019; and Yi Dai Yi Lu Zhongguo

connections and potential corruption allegations, there is no evidence indicating that CCCCL has military connections or is involved in "defense or related materiel" businesses.

China National Offshore Oil Corporation (CNOOC)

China National Offshore Oil Corporation is a super-large SOE established by the State Council in 1982, and currently majority-controlled by SASAC. It is China's largest offshore oil and gas production operator. The company has assets of RMB 721.3 billion (US$ 113.6 billion) and controls 65% of the shares of its subsidiary CNOOC Limited, which is listed on the Hong Kong and Toronto Stock Exchanges, and was previously on the New York Stock Exchange prior to being de-listed in March 2021 as a result of Trump's executive order.[71]

CNOOC's main business segments include oil and gas exploration and development, professional technical services, refining and sales, natural gas and power generation, and financial services. In 2020, CNOOC ranked 64th on the "Global Fortune 500 Companies" list and 30th among the "World's 50 Largest Oil Companies" as selected by *Petroleum Intelligence Weekly* (PIW).[72]

While CNOOC is essential to China's economic development as its largest offshore oil and gas production and development corporation, there is no evidence indicating CNOOC's military connections or involvement in "defense or related materiel." So its inclusion on Trump's tranche 4 list of CCMCs in late 2020 caused much controversy and further incited China-U.S. tensions.[73]

Besides the highly awkward fact that none of these three SOEs has any obvious "defense or related materiel" connections, there are other factors that challenge the legitimacy of Biden's list. First, two large Chinese SOE construction firms that were previously on Trump's Tranche 4 list were removed by Biden in June 2021, namely China Construction Technology Co. Ltd. (CCTC), and China International Engineering Consulting Corp. (CIECC). Their profiles are very similar to CRCC and CCCCL, being involved in major civilian government-funded construction projects.[74] The continued inclusion

Qiye 100 Qiang Mingdan (一带一路中国企业100强名单) [*Belt and Road Top 100 Chinese Enterprises List* (2019)], Economic News Daily, http://www.nbd.com.cn/articles/2019-11-13/1386031.html.

[71] CNOOC Ltd., *Company Profile*, https://www.cnoocltd.com/col/col7261/index.html (accessed March 30, 2023); CNOOC Ltd., Annual Report (Form 20-F), 102 (filed with SEC on April 22, 2021); and CNOOC Ltd., *2020 Annual Report*, 29, 34 (Apr. 8, 2021), https://www.cnoocltd.com/attach/0/c63efe2e72b84001bf234fcc38d836ff.pdf. The de-listing resulted from CNOOC Ltd. and its parent CNOOC being added to the 4th tranche of companies on Trump's list of CCMCs.

[72] CNOOC Ltd., *Gongsi Jianjie* (公司简介) [*Corporate Profile*], https://www.cnooc.com.cn/col/col661/index.html (accessed March 30, 2023).

[73] Alexandra Alper & Humeyra Pamuk, *Exclusive: Trump to Add China's SMIC and CNOOC to Defense Blacklist*, REUTERS (Nov. 30, 2020), https://www.reuters.com/article/us-usa-china-military-companies-exclusiv-idUSKBN28A036; and The White House, *Tranche 4 - Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (PUBLIC LAW 105–261)* (December 2020), https://media.defense.gov/2020/Dec/03/2002545864/-1/-1/1/TRANCHE-4-QUALIFYING-ENTITIES.PDF (hereafter "Tranche 4 list").

[74] For profile of CCTC, *see* CCTC, *Group Overview*, https://www.cctc.cn/jtgk/qyjj/index.shtml; and for CIECC, *see* CIECC, *About CIECC*, http://en.ciecc.com.cn/col/col3226/index.html (last visited July 17, 2023).

of the latter two companies on Biden's list juxtaposed to the removal of the former reveals a strange inconsistency of treatment by the U.S. government. Second, if CNOOC is considered to be a company in "defense or related materiel" solely because it is a major offshore oil and gas producer for China, why is it that China's two much larger domestic oil producers, CNPC and Sinopec, have not been placed on the list?[75] The criteria for including these large SOEs on Biden's list are as unclear and inconsistent as they were for Trump's lists.

b. Telecommunications Service Companies. All three of China's key SOE telecom service providers are included in Group 1 as "defense or related materiel" companies (and their main parent or subsidiary companies are included in Group 3 as companies controlling or controlled by these entities).

They are:

(1) China Telecommunications Corporation (China Telecom),

(2) China United Network Communications Group Co., Ltd (China Unicom)

(3) China Mobile Communications Group Co., Ltd. (China Mobile)

As with CRCC and CCCCL, these three telecom companies are central government-controlled SOEs with large proportions of their shares held by SASAC, and they all have listed companies as part of their corporate group. China Telecom's subsidiary is listed on the Hong Kong and Shanghai Stock Exchanges;[76] China Unicom's subco is on the Shanghai Stock Exchange;[77] and China Mobile's subco was listed in both Hong Kong and New York Stock Exchange prior to its de-listing from the latter as a result of being placed on Trump's list.[78]

There is no direct evidence showing that these three telecom companies have any strong connections with the military. Information available on their company websites and in stock exchange public announcements strongly indicates that the primary business of all these companies is to provide telecom and internet products and services to consumers and businesses. For example, China Unicom recorded 47.23% of its 2021 revenue from its broadband and mobile data services, 6.85% from telecom monthly rental and voice services; 18.95% from its internet application services; and 9.44% from its sales income

[75] For Sinopec, *see* SINOPEC, *About Us*, http://www.sinopecgroup.com/group/en/gywm/about.shtml (accessed March 30, 2023); ; and for CNPC, *see* CNPC, About *CNPC*, https://www.cnpc.com.cn/en/aboutcnpc/aboutcnpc_i ndex.shtml (accessed March 30, 2023).

[76] By Jan 2022, the State shareholding in China Telecom accounted for 63.2%: *see* China Telecom, *Konggu Jiegou* (控股结构) [*Shareholding Structure*], https://www.chinatelecom-h.com/sc/company/structure.php.

[77] By April 2021, the State shareholding in China Unicom accounted for 79.9%: *see* China Unicom, *Guquan Jiegou* (股权结构) [*Shareholding Structure*] http://www.chinaunicom.com.cn/about/structure.html (accessed March 30, 2023).

[78] By the end of 2021, the State shareholding in China Mobile accounted for 72.72%: *see* China Mobile, *Guquan Jiegou* (股权结构) [*Shareholding Structure*], https://www.chinamobileltd.com/sc/ir/shareholdingstructure.php (accessed March 30, 2023).

of standard telecom devices.[79] The reason for including these companies in Group 1 is therefore unclear.

When tracing the history and development of these companies, it is clear that they have consistently held a special status as monopoly telecom providers. They emerged out of the state telecom ministry or other government ministries, and the way that they were corporatized as SOEs and subsequently listed was carefully orchestrated by the government to maintain state control over this critical communications infrastructure. All three companies enjoy special policy privileges, and in return, they had to assist with developing China's communications networks in rural regions, even if this was not always profitable. Clearly, they are backed by the State and continue to play an important role in the PRC's national development, such as the recent construction of smart cities and their 5G networks. However, we have not located any evidence to justify their inclusion as "defense or related materiel companies."

There is no doubt that these three companies or their subsidiaries supply telecom and internet services to the Chinese military. Otherwise, the military would need to rely on a foreign supplier, which would create national security risks for China itself. One 2021 report by RWR Advisory Group, a Washington, DC-based "risk and threat consultancy," lists several examples, most of which appear to be standardized communications equipment or telephone networks supplied to military customers in different parts of China.[80]

The question is whether a civilian company whose business is primarily based on supplying services to the Chinese retail and business market, and as part of that business also supplies standardized services that are used by the Chinese military, should be sanctioned by the U.S. government. We should add here that these three telecom firms have also recently had their licenses to offer telecom services in the U.S. revoked by the Federal Communications Commission due to alleged "national security concerns."[81] Is this designed to protect U.S. national security or, more likely, to engage in disguised economic protectionism, limiting their access to foreign capital and harming ordinary Chinese consumers by making it difficult to access roaming services with their home provider overseas? Is the alleged security risk – which so far appears to be potential rather than actually proven – really so great that it justifies preventing U.S. investors from sharing in the profits of an expanding Chinese economy through these companies?

---

[79] China Unicom, *Business structure and analysi*s, Shanghai Exchange Data Centre (2021), *available at* http://emweb.securities.eastmoney.com/PC_HSF10/BusinessAnalysis/Index?type=web&code=SH600050# (accessed March 30, 2023).

[80] RWR Advisory Group, *Military Ties of Major Chinese State-Owned Telcom Companies: China Mobile, China Unicom, China Telecom*, JANES INTELTRAK (Feb. 2, 2021), https://www.rwradvisory.com/wp-content/uploads/2021/02/RWR_China_Telco_CCMCs.pdf.

[81] For discussion of all three Chinese SOE telecom firms, see David Shepardson, *FCC revokes authorization of China Telecom's U.S. unit*, REUTERS, Oct. 27, 2021, https://www.reuters.com/business/media-telecom/fcc-votes-terminate-china-telecom-americans-authority-provide-us-services-2021-10-26/.

Moreover, if the criterion for including these three telecom firms on the list is that they supply services to the military and are considered strategically important to the Chinese economy, then why not include the rest of China's ninety-seven centrally-controlled SOEs administered by SASAC, as all of them would supply some kinds of products or services to the military to a greater or lesser degree?[82]

c. Electronics Company

Semiconductor Manufacturing International Corporation (SMIC)

SMIC is one of the world's largest chip makers. Besides being the biggest multinational integrated circuit manufacturing enterprise group in China, it also provides foundry and technical services.[83] SMIC operates on a global scale, with about 58% of its business income coming from the Chinese market, 25% from the North American market, and the rest from Europe and other parts of Asia.[84]

Former President Trump included SMIC on the list of defense companies in his tranche 4 release, which led to extensive media debate and escalated intergovernmental tensions.[85] Though little explanation was provided, the U.S. Commerce Department had previously informed some U.S. firms that they needed to obtain a license before supplying goods and services to SMIC after concluding there was an "unacceptable risk" that equipment supplied to it could be used for military purposes.[86] On the same day as the tranche 4 list was released, SMIC made two public announcements, stressing that the company manufactures semiconductors and provides services solely for civilian and commercial clients. "The company has no relationship with the Chinese military and does not manufacture for any military end-users or end-uses," read the announcement.[87]

Whatever the merits of this statement, with regard to its share ownership, SMIC is actually a Cayman Islands company listed on both the Shanghai and Hong Kong Stock Exchanges. Approximately 13% of its shares are held by Chinese state-owned institutional shareholders, and the largest of these, holding

[82] *List of companies directly owned and controlled by the State Council*, SASAC (2022), http://en.sasac.gov.cn/directorynames.html]; Yi Zhang, *Consultation on the definition of state-owned enterprises and enterprises on SASAC list*, SASAC (Nov. 24, 2017, 8:50 AM), http://www.sasac.gov.cn/n2588040/n2590387/n9854207/c9933656/content.html.

[83] *Company Summary*, SEMICONDUCTOR MANUFACTURING INTERNATIONAL CORPORATION (2022), https://www.smics.com/site/about_summary.

[84] *Main business composition analysis*, SHANGHAI STOCK EXCHANGE (2022), http://emweb.securities.eastmoney.com/PC_HSF10/BusinessAnalysis/Index?type=web&code=sh688981.

[85] *The US puts SMIC and other Chinese companies on the blacklist of the so-called 'military industrial enterprises': PRC Ministry of Foreign Affairs: Resolutely opposed*, XINHUA NET (Dec. 4, 2020) http://www.xinhuanet.com/world/2020-12/04/c_1126822990.html; *see also* Alexandra Alper & Humeyra Pamuk, *Exclusive: Trump to add China's SMIC and CNOOC to defense blacklist*, REUTERS (Nov. 30, 2020), https://www.reuters.com/article/us-usa-china-military-companies-exclusiv-idUSKBN28A036.

[86] Alper & Pamuk, *supra* note 86.

[87] SMIC, *SMIC's follow-up announcement on concerned matters*, SHANGHAI STOCK EXCHANGE (Dec. 4, 2020), https://pdf.dfcfw.com/pdf/H2_AN202012041436541301_1.pdf?1607085097000.pdf.

12.1%, is a central government SOE administered by SASAC. However, the majority of its shares are held by members of the public through the Hong Kong Stock Exchange.[88]

Though SMIC certainly has some minority state investment, it clearly operates as a publicly listed commercial business manufacturing and selling semiconductor chips in China and throughout the world. We could not locate any evidence showing that the company has military or defense-related links or operations.[89] Most U.S. commentary seems to focus much more on the potential for SMIC and other Chinese semiconductor manufacturers to somehow leverage advances in chip technology to undermine the international technological industry, though without clearly specifying how this would happen. A recent article by Hannah Kelley provides a typical example of this kind of vague prognostication:[90]

"Today's greatest threat to the global chip industry—and to the balance of strategic technology competition at large—is an authoritarian China's pursuit of technological dominance. As a gatekeeper to semiconductor chips, China would have a steel toe boot in the door for other chip-enabled critical technologies, including robotics and quantum computers. Such power would position Beijing to set standards and norms promoting global technological authoritarianism, where it stands to gain in absolutes."

Based on the available evidence, SMIC's inclusion on Trump's and Biden's lists is, therefore, more likely due to it being a potential future competitor to American and other multinational firms in semiconductors, a technology that the U.S. government views as strategically important. Its situation is similar to Xiaomi and Luokung in their respective sectors of 5G and AI, which were also claimed to be strategic areas by the Department of Defense, without further proof that those companies were actually linked to the Chinese military or surveillance industries.

---

[88] This SOE is called 中国信息通信科技集团有限公司 (China Information Communications Technology Group Ltd. or CICT). *See 2020 Nian Niandu Baogao* [2020 Annual Report], SMIC (Apr. 28, 2020), at 7, 93, https://www.smics.com/uploads/2.2020&e5&b9&b4&e5&b9&b4&e5&ba&a6&e6&8a&a5&e5&91&8a-A%20cn.pdf; *CICT*, Qichacha (Baidu Credit), https://aiqicha.baidu.com/company_detail_10692751464354.

[89] Brunner and Weinstein state that several of SMIC's subsidiaries are on the Pentagon's Section 1260H list (another U.S. government sanctions list) "because they are connected to the Chinese military," but the Pentagon does not include any explanation or evidence for placing these firms on the list, so it is difficult to know what the justification is beyond them being in the strategically important industry sector of semiconductors. *See* Jordan Brunner & Emily Weinstein, *The Strategic and Legal Implications of Biden's New China Sanctions*, LAWFARE (Jun. 18, 2021), https://www.lawfareblog.com/strategic-and-legal-implications-bidens-new-china-sanctions; and U.S. Department of Defense, *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)* (Jun. 3, 2021), https://media.defense.gov/2021/Jun/03/2002734519/-1/-1/0/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-US.PDF.

[90] Hannah Kelley, *Where the U.S. Chips Fall: Fault Lines and Big Breaks in the Global Semiconductor Industry*, GEORGET. J. INT. AFF. (Feb. 17, 2022), https://gjia.georgetown.edu/2022/02/17/where-the-u-s-chips-fall-fault-lines-and-big-breaks-in-the-global-semiconductor-industry/.

True, if SMIC continues to improve its innovative capabilities, the company may eventually learn to compete with global leaders, but currently, it is still "two or three generations behind," unable to produce "most cutting-edge chips for computer, smartphone, and server processors … [or for] high-performance computing." By contrast, U.S. suppliers are still dominant, "controlling more than 80% of the market" in several specialized semiconductor equipment segments "necessary for building advanced chips."[91] And even if SMIC could somehow catch up with U.S. firms over the next decade, to sanction the firm by claiming that it is involved in "defense and related materiel" is to stretch the definition of those terms to breaking point.

d. Companies Included in Both Groups 1 and 2: Hikvision and Huawei. There are two other companies listed in Group 1 whose "defense and related materiel" links are not clear: Hikvision and Huawei. Both these companies also appear in Group 2 as "surveillance technology" firms, so it is necessary to discuss them in relation to both these industry sectors.[92]

Huawei Technologies Co., Ltd. (Huawei)

Much ink has been spilled, and several government investigations have been held on the alleged "potential security threat" posed by Huawei to the U.S. and its allies, as well as its claimed "military links." Yet hard evidence against the company is surprisingly thin. Space does not permit a detailed examination of this evidence, but here we will focus on the issue of whether Huawei's inclusion on Biden's list is clearly justified.

As the world's largest seller of smartphones and telecommunications equipment, including 5G network infrastructure, Huawei is a private enterprise owned by its employees. Its early success came through being able to offer durable telecom and internet hardware at significantly lower cost than multinational and Chinese state-owned firms, and to back this up with excellent customer service. More recently, its long-term strategy of plowing at least 10% of its annual revenues into R&D has made it one of the largest invention patent holders in the world, and a leader in several 5G technologies.[93]

Citing potential national security risks, Australia, India, Canada, the United States, and other countries have effectively banned Huawei from building their 5G networks, though many other countries continue to do business with the company.[94]

---

[91] Cheng Ting-Fang & Lauly Li, *China's SMIC stockpiles chip equipment to counter US restrictions*, NIKKEI. AS. R. (Sep. 30, 2020), https://asia.nikkei.com/Politics/International-relations/US-China-tensions/China-s-SMIC-stockpiles-chip-equipment-to-counter-US-restrictions.

[92] *Supra* note 38, for the double categorization in groups 1 and 2, see "White House Fact Sheet."

[93] For Huawei's development, see YUN WEN, THE HUAWEI MODEL: THE RISE OF CHINA'S TECH GIANT (1st ed. 2020).

[94] For Australia, Stephen McDonell, *China criticizes Government's decision to uphold NBN ban on telco Huawei*, ABC LATELINE (Oct. 30, 2013), http://www.abc.net.au/news/2013-10-29/china-angered-by-decision-uphold-nbn-ban-on-huawei/5056588; for India, Mehal Srivastava & Mark Lee, *India Said to Block Orders for ZTE, Huawei Technologies Telecom Equipment*, BLOOMBERG (Apr. 30, 2010),

In terms of whether it is a company in the "defense or related materiel" sector (Group 1), the main evidence presented by the U.S. government is that Huawei's founder and CEO, Ren Zhengfei, was an officer in the Chinese People's Liberation Army (PLA) for many years and that the military continues to influence Huawei's business both as an important customer and a financial backer of the firm.[95] However, these claims have very shaky evidential foundations.

Indeed, Huawei's CEO Ren Zhengfei was once a relatively low-ranking officer in the Chinese military engineering corps.[96] But he left the army in 1983, and a few years later in 1987 set up a small private business selling simple telephone exchange switches imported from Hong Kong, which later grew into Huawei.[97] There is no convincing evidence that Ren Zhengfei maintained any close connections with the Chinese military or that the military has exercised any influence over Huawei's business.

The story about Huawei's military ties appears to have been sparked by Bruce Gilley, then a reporter from the newsweekly *Far Eastern Economic Review*, who visited Huawei's Shenzhen manufacturing facility back in 2000. He claimed to have come across three large telephone exchange switches in Huawei's shipping warehouse addressed to the telecom bureau of the People's Liberation Army (PLA).[98] Unfortunately, the article did not provide any photographic evidence or details of the equipment's specifications. The only other hard evidence was a comment by Huawei's Senior Vice President Fei Min that the company did sell some standardized equipment to the Chinese military at that time, but it made up less than 1% of the company's overall sales.[99] From this, the reporter concluded that Huawei was a "military-backed company."[100]

http://www.bloomberg.com/news/2010-04-30/india-said-to-block-china-s-huawei-zte-from-selling-phone-network-gear.html; and for Canada, Steven Chase, *Ottawa set to ban Chinese firm from telecommunications bid*, THE GLOBE AND MAIL (Oct. 10, 2012), http://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/.

[95] M. Rogers & D. Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, US HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE (Oct. 8, 2012), pp. vi–vii, https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96 [hereafter *PSC Report*], pp.13–14, 21–22, 24–25.

[96] *See PSC Report*, at 24.

[97] *See* ZHANG GUANJING (张贯京), HUAWEI SI ZHANG LIAN (华为四张脸) [HUAWEI'S FOUR FACES] 23–24, 135, 223–24 (2017).

[98] *See* Bruce Gilley, *Huawei's Fixed Line to Beijing*, *FAR E. ECON. REV.* 94, 94–98 (2000) [hereafter *Gilley*].

[99] *Id.* at 96. Gilley also cited unnamed "foreign analysts" and a Russian assistant manager at Huawei's Moscow office to back up his claims of Huawei's "military ties," none of whom seemed to have close access to Huawei. Huawei has never denied that one of its customers is the Chinese military, but has consistently maintained that such military sales have never made up more than 1% of its overall sales. With the growth of its overall business, sales to the Chinese military now make up only 0.1% of its overall sales, according to statements provided by Huawei to the Congressional Permanent Select Committee: *see PSC Report*, p.34.

[100] *See Gilley*, p.94.

Such a speculative news article would normally have disappeared quickly, but it gained a new lease of life in an influential 2005 report by the RAND Corporation with the imposing title *A New Direction for China's Defense Industry*.[101] The RAND report claimed that Huawei was part of a new "digital triangle" between the Chinese state, military, and commercial IT industry and that "Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner."[102] Unfortunately, the only named source cited for these assertions is the same *Far Eastern Economic Review* article from 2000 – which, even at face value, does not support such wide-ranging conclusions about "deep ties," military patronage, or R&D partnerships.[103]

Many of the media reports and government committees that continue to raise these allegations about Huawei's "military ties" cite this RAND Report without questioning the paucity of its source material.[104] It is even relied on in the Congressional Permanent Select Committee on Intelligence Report as the main "evidence" by "many analysts" of Ren Zhengfei's continuing military connections, and this Committee's report was later cited by the U.S. Federal Communications Commission as justification for banning U.S. telecom providers from using Huawei's equipment in their networks.[105] If this is the best evidence that a well-funded U.S. congressional intelligence committee can dig out for Huawei's military ties, the substance of these allegations is highly doubtful.[106]

In terms of whether Huawei is in the "surveillance technology" sector (Group 2), the U.S. government has alleged that Huawei's network equipment could be used to transmit sensitive information back to the Chinese government and that Huawei would not be able to refuse demands by the Chinese security and intelligence services to cooperate with such espionage activities. This does not mean that Huawei is producing surveillance technology as such, but rather that its equipment installed in the U.S. and other countries may have been, or potentially will be, compromised to allow surveillance and cyberattacks to

[101] EVAN S. MEDEIROS, ROGER CLIFF, KEITH CRANE & JAMES C. MULVENON, A NEW DIRECTION FOR CHINA'S DEFENSE INDUSTRY (2005).

[102] *Id*. at 218.

[103] MEDEIROS ET AL., *supra* note 103, at 219–21, the report also refers to some unnamed "interviewees" in Beijing, which is a long distance from Huawei's headquarters in Shenzhen.

[104] *E.g.*, J. Dean, *Outside of U.S., Few Fear Huawei*, WALL ST. J. (ASIAN EDITION), Feb. 22, 2008; Tech Law Journal, *3Com Huawei transaction to be reviewed by CFIUS*, TECH. L. J. (Oct. 9, 2007), http://www.techlawjournal.com/topstories/2007/20071009b.asp.

[105] PSC Report, at 13 and 48. For Huawei's unsuccessful appeal against the FCC's banning order, in which the judge mentions the PSC Report, *see* Huawei Techs. USA, Inc. v. FCC, 2 F.4th 421, 4 (5th Cir. 2021).

[106] PSC Report (at 10) also refers to a "classified annex" that the writers claim contains much more evidence against Huawei, but this cannot be published due to "national security concerns." We discuss the issue of classified information further below.

occur, which threatens U.S. national security.[107] Huawei, of course, has denied these claims and insisted that its network equipment is secure and that it works with overseas governments and telecom firms from the 140-plus countries that have purchased its products to ensure that they are secure from any unwanted intrusions.[108]

It may not be possible to definitively answer the question of whether Huawei's network equipment poses a "potential" national security threat. What is interesting about the various investigations of Huawei conducted by numerous countries is that none have uncovered any clear evidence of the company assisting the Chinese government to engage in espionage or seeking to undermine the security of foreign governments.[109] The UK government has

[107] PSC Report, at 3 ("It appears that under Chinese law, ZTE and Huawei would be obligated to co-operate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state security.").

[108] *See*, *e.g.*, Charles Ding, *Written Statement for Charles Ding, Corporate Senior Vice President, Huawei, to the Permanent Select Committee on Intelligence,* U.S. HOUSE OF REPRESENTATIVES (Sept. 13, 2012), https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/091312huaweitestimony.pdf.

[109] Of the two U.S. criminal cases currently under way against Huawei, neither is a national security issue unless one expands the definition of national security to include alleged economic crimes against corporations, some of which are not even U.S.-based: one is an allegation of bank fraud committed by Huawei against HSBC and Standard Chartered Bank in relation to Huawei's business in Iran, but so far no breach by Huawei or its affiliates of U.S. sanctions against Iran has been proven, and there are exceptions to the sanctions that allow for sales of civilian-use internet hardware in Iran that may protect Huawei. Other multinationals, such as Nokia and Ericsson, have also taken advantage of these exceptions to sell telecom equipment in Iran, for which see Christopher Rhoads & Loretta Chao, *Iran's Web Spying Aided By Western Technology*, WALL S. J. (June 22, 2009), https://www.wsj.com/articles/SB124562668777335653; and for Ericsson, *see* Steve Stecklow, *Exclusive: Ericsson Helps Iran Telecoms, Letter Reveals Long-Term Deal*, REUTERS (Nov. 20, 2012), http://www.reuters.com/article/2012/11/20/us-iran-ericsson-idUSBRE8AJ0IY20121120. The fraud allegations against Huawei are based on a single ambiguous powerpoint presentation, *see* U.S. v. Huawei Technologies Co., Ltd. et al., Superseding Indictment, Cr. No. 18-457 (S-2) (AMD) (E.D.N.Y.), https://www.justice.gov/opa/press-release/file/1125021/download; and Ian Young, *This PowerPoint presentation proves Huawei CFO Sabrina Meng Wanzhou Is Guilty, says US. Preposterous, says Her Lawyer*, S. CHINA MORNING POST (Dec. 18, 2018), https://www.scmp.com/news/china/diplomacy/article/2178250/powerpoint-presentation-proves-huawei-cfo-sabrina-meng-wanzhou. The second case involves trade secrets allegedly "stolen" by Huawei for its own use from T-Mobile, an issue that was already decided in civil proceedings back in 2017, but has now been resurrected as a criminal case, see U.S. v. Huawei Device Co. Ltd. et al., Indictment, CR19-010 RSM (W.D. Wash.), https://www.justice.gov/d9/press-releases/attachments/2019/01/28/huawei_indictment_pacer_0.pdf; and Mike Dano, *T-Mobile Wins $4.8M Ruling Against Huawei Over Alleged Theft Of Smartphone-testing Robot 'Tappy'*, FIERCE WIRELESS (May 22, 2017), https://www.fiercewireless.com/wireless/t-mobile-wins-4-8m-ruling-against-huawei-over-alleged-theft-smartphone-testing-robot-tappy. Incidents have allegedly occurred elsewhere, in Poland and Africa, but the details are sketchy, and so far no person has been convicted of any espionage charges, see Joanna Plucinska et al., *How Poland Became a Front in the Cold War Between the U.S. and China*, REUTERS (July 2, 2019), https://www.reuters.com/investigates/special-report/huawei-poland-spying/; Huawei Technologies, *Court orders Lithuanian news outlet to retract false statements on Huawei* (Oct.11, 2019), https://www.huawei.com/en/facts/voices-of-huawei/court-orders-lithuanian-news-outlet-to-retract-false-statements-on-huawei; and Salem Solomon, *After Allegations of Spying, African Union Renews Huawei Alliance*, VOICE AM. NEWS (June 7, 2019), https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html#:~:text=With%20criticisms%20mounting%20around%20the,to%205G%20and%20artificial%20intelligence.

conducted the most intense scrutiny of Huawei's telecom and network equipment, with continuous testing by independent technical experts since 2003 through the Huawei Cyber Security Evaluation Centre (HCSEC). The Centre's annual reports have scathingly criticized some vulnerabilities in Huawei's products, and the need for the company to remediate defects in its software engineering and cyber security processes in order to prevent potential security risks.[110] Despite these serious flaws, the most recent HCSEC Report concluded: "NCSC does not believe that the defects identified are a result of Chinese state interference."[111] In other words, the UK Government's National Cyber Security Centre, which oversees HCSEC and has a duty to protect UK citizens from cyber risks, has not detected any Chinese government/military "interference" in any of Huawei's hardware or software that is used in the UK.

Likewise, in a remarkably detailed April 2019 investigation of the company by the *Los Angeles Times*, the reporters concluded:[112]

None of the U.S. intelligence officials interviewed over several months for this story have made information public that supports the most damning assertions about China's control over Huawei and about Ren's early ties to Chinese military intelligence. They have yet to provide hard evidence and, privately, these officials *admit they don't have any*.

Making a "potential" rather than an actual threat the criterion for sanctioning Huawei and preventing U.S. entities from investing in it is highly problematic for several reasons. First, it once again displays inconsistency, as Huawei's main Chinese competitor ZTE is not included on Biden's list due to its settlement with the U.S. government, even though it was equally identified as a potential security threat by the US Congress in its 2012 investigation.[113] Second, a "potential threat" test would also encompass the majority of multinational network equipment manufacturers, software operating system providers, and internet browsers – such as Microsoft, Apple, Google, and Cisco Systems, as all of them regularly experience cyber hacking, some of which is allegedly directed by foreign governments, and this has resulted in serious disruption to American government institutions and critical infrastructure and caused huge economic losses to U.S. businesses and consumers.[114] Finally,

[110] Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board, *Annual Report 2019: A report to the National Security Adviser of the United Kingdom* (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[111] *Id.* at 21.

[112] My emphasis. Norman Pearlstine et al, *The Man Behind Huawei*, L. A. TIMES (Apr. 10, 2019), https://perma.cc/EQL3-W2RB.

[113] *See supra* note 97; and Jonathan C. Poling et al., *Commerce Department Signs New Agreement with ZTE Lifting Denial Order in Exchange for Unprecedented Additional Penalties and Compliance Measures*, AKIN (June 12, 2018), https://www.akingump.com/en/insights/alerts/commerce-department-signs-new-agreement-with-zte-lifting-denial.

[114] For just a few recent examples, see Kif Leswing, *Apple iPhones can be hacked with spyware even if you don't click on a link, Amnesty International says*, CNBC (Jul. 19, 2021), https://www.cnbc.com/2021/07/19/apple-iphones-can-be-hacked-even-if-the-user-never-clicks-a-link-

allowing an American president to sanction or even ban a company purely due to a "potential threat" sets a dangerous precedent that could be abused for personal gain. This may have already occurred with former President Trump's attempted ban of the video streaming company TikTok in 2020, which several commentators attributed to Trump's anger at TikTok users organizing boycotts of his campaign rallies rather than national security concerns.[115]

To sum up, the evidence against Huawei is surprisingly weak in both the defense and surveillance categories, and its inclusion on Biden's list reveals a mix of inconsistent and arbitrary criteria applied by the U.S. government similar to those we have identified above with other corporations on the list.

Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision)

Space does not permit a detailed discussion of Hikvision, another private firm, but Hikvision's inclusion on the sanctions list in both Groups 1 and 2 appears to be primarily due to its surveillance camera technology used by civilian police and security forces within China, rather than any military connections.[116] However, it is not clear why domestic Chinese surveillance of its own citizens would be a "national security threat" to the United States.

Moreover, if the test for bringing sanctions on international companies is that their products/services have been or may be used for intrusive surveillance by foreign governments or police forces, this would capture numerous non-

amnesty-international-says.html; Lily Hay Newman, *'This Is really, really bad': Lapsus$ Gang claims Okta hack*, WIRED (Mar. 22, 2022), https://www.wired.com/story/okta-hack-microsoft-bing-code-leak-lapsus/; Joseph Menn, *Microsoft says new breach discovered in probe of suspected SolarWinds hackers*, REUTERS (Jun. 28, 2021), https://www.reuters.com/technology/microsoft-says-new-breach-discovered-probe-suspected-solarwinds-hackers-2021-06-25/; Catalin Cimpanu, *Hackers have started attacks on Cisco RV110, RV130, and RV215 routers*, ZDNET (Mar. 3, 2019), https://www.zdnet.com/article/hackers-have-started-attacks-on-cisco-rv110-rv130-and-rv215-routers/; Dan Milmo, *Google warns of surge in activity by state-backed hackers*, THE GUARDIAN (Oct. 15, 2021), https://www.theguardian.com/technology/2021/oct/15/google-warns-surge-activity-state-backed-hackers; and Stephanie Kelly and Jessica Resnick-ault, *One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators,* REUTERS, (Jun. 9, 2021), https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.

[115] Abram Brown, *Is This The Real Reason Why Trump Wants To Ban TikTok?*, FORBES (Aug. 1, 2020), https://www.forbes.com/sites/abrambrown/2020/08/01/is-this-the-real-reason-why-trump-wants-to-ban-tiktok/?sh=414afffa4aed; and contrast Scott Nover, *Biden is Taking Trump's Argument Against TikTok Seriously,* VOX (Jun. 22, 2021), https://qz.com/2023128/after-trumps-ban-failed-biden-gives-tiktok-a-second-look/. Citizen Lab, a Toronto-based independent technology investigative thinktank, found that there was no evidence TikTok posed any national security threat or had shared any data with the Chinese government: *see TikTok and Douyin Explained*, THE CITIZEN LAB (Mar. 22, 2021), https://citizenlab.ca/2021/03/tiktok-and-douyin-explained/.

[116] For a clear analysis of the U.S. government's motivations, *see* Jon Batemen, *U.S. Sanctions on Hikvision Would Dangerously Escalate China Tech Tensions*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (May 6, 2022), https://carnegieendowment.org/2022/05/06/u.s.-sanctions-on-hikvision-would-dangerously-escalate-china-tech-tensions-pub-87089. For the company's businesses, *see* Hangzhou Hikvision Digital Technology Limited (2022), *Gongsi Jianjie (Corporate Profile)*, https://www.hikvision.com/cn/aboutus/CompanyProfile/; and HANGZHOU HIKVISION DIGITAL TECHNOLOGY LIMITED (2022), *2020 Nian Niandu Baogao* (*2020 Annual Report)*, https://www.hikvision.com/content/dam/hikvision/cn/about-us/financial-report/report/2020Q4.PDF (last updated Apr. 17, 2021).

Chinese corporations too. To give just one highly relevant example, according to a detailed expose by investigative reporter Mara Hvistendahl, the U.S. multinational database solutions firm Oracle Corporation has sold its big data analytic software systems to several public security (i.e. police) forces in China, and there is little doubt that they have been used for similar kinds of surveillance operations as those involving Hikvision's video cameras.[117] Logically speaking, this should mean that Oracle should be added to Biden's list, with the result that U.S. entities should be prohibited from purchasing its stocks, and it should be de-listed from U.S. securities exchanges.

The example of Hikvision once again reveals an arbitrary inconsistency in the U.S. government's application of sanctions to corporations engaging in similar kinds of behavior, and it also appears to confuse two separate issues that should be clearly distinguished, namely, military/national security threats to the U.S. and the Chinese government's domestic surveillance activities.

C. Companies in Group 3: Parent and Subsidiary Corporations

Group three of Biden's list consists of ten corporations that either control or are controlled by other corporations on the list: see Appendix, Table 3. The inclusion of these affiliated corporations is presumably to try and prevent U.S. investors from investing in a parent or subsidiary Chinese corporation to avoid the sanctions, which would effectively make a list redundant.

While the idea of including parent and subsidiary corporations may be a sound one, its execution is extremely random, leading to numerous gaps and inconsistencies. One commentary by Brunner and Weinstein notes that some key subsidiaries of defense corporations are missing from the list despite actively operating outside China, such as China National Aero-Technology Import & Export Corporation (CATIC), a subsidiary of AVIC,[118] which is omitted even though AVIC itself and several other AVIC-affiliated corporations are listed.

More broadly, the Frequently Asked Questions provided by the U.S. government's Office of Foreign Assets Control (OFAC) make it clear that a subsidiary is covered by the new sanctions only if the exact name of the subsidiary is itself on the list; there is no "general control" test that would automatically make subsidiaries of the listed companies subject to the sanctions if they are not separately listed.[119] This would greatly dilute the reach of the sanctions because virtually all the corporations on Biden's list have dozens or

[117] Mara Hvistendahl, *How Oracle Sells Repression In China*, THE INTERCEPT (Feb.18, 2021), https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

[118] Brunner and Weinstein, *supra* note 38.

[119] *See* FAQs 857 and 899, Office of Foreign Assets Control, U.S. Treasury Department (OFAC), *OFAC Consolidated Frequently Asked Questions*, https://home.treasury.gov/policy-issues/financial-sanctions/frequently-asked-questions/ofac-consolidated-frequently-asked-questions; and useful analysis by John E. Smith, Brandon L. Van Grack, B. Chen Zhu and Panagiotis C. Bay, *Sanctions on Chinese Military and Surveillance Companies*, Morrison & Foerster LLP, (Jun. 8, 2021), https://www.mofo.com/resources/insights/210608-biden-issues-executive-order.html.

even hundreds of subsidiaries and affiliated companies which are not included. Also, there is nothing to prevent a Chinese corporation that is listed from setting up a new subsidiary with a different name and then using it to raise money from investors, including potentially U.S. investors who purchase shares in Hong Kong or Mainland China. The U.S. government may catch up with them over time, but it is a cumbersome process to keep adding names of new subsidiaries to the list.

Of course, other U.S. government sanctions may cover these kinds of "controlled entities" and subject them to export bans or financial blocks,[120] but this begs the question as to the utility of Biden's list at all, especially when one takes into account the various other defects identified earlier.

V. CONCLUSION

This paper has identified various continuing defects with Biden's list of Chinese defense and surveillance technology corporations, some of which were inherited from the Trump administration lists and others of which are new. Problems include apparently arbitrary criteria for including or removing corporations from the list; a failure to clearly explain why some corporations with no apparent military links are placed in the "defense and related materiel" group; over-broad definitions that could easily ensnare U.S. corporations if consistently applied; mixed objectives that confuse U.S. national security with involvement in domestic Chinese governance issues; inconsistency with other U.S. government entity lists that also focus on national security or human rights, leading to an opaque melange of sanctions that would be difficult for any corporation to locate and comply with; and major gaps and loopholes that indicate the preparation of the list was a hasty and slapdash process and would hamper its implementation.

It may be that the U.S. government is justified in seeking to minimize financial support for Chinese military corporations by U.S. investors due to the increasing strategic tensions between these two nations.

However, if the justification for such actions is that the Chinese government is "breaking trust at home and abroad, rejecting property rights and predictable rule of law," in Mike Pompeo's words, the U.S. government must itself act in a predictable, lawful, non-capricious way to demonstrate what abiding by rule of law actually means in practice. The cases of *Xiaomi* and *Luokung* already revealed that the selection of some corporations was not based on justifiable reasons or rational grounds, and as we have shown, the inclusion of almost 20% of the other corporations that remain on Biden's list cannot be clearly justified

[120] Other sanctions lists include the Department of Commerce's entity lists making it illegal to export U.S. products to those entities; lists relating to companies that allegedly have supported the repression in Xinjiang; bans on specific companies selling their products to U.S. government bodies; and what appears to be a "name and shame" list produced by the Pentagon under s.1260 of the NDAA. See *supra* note 4 for citations.

on "national security" grounds, based on available open access sources.[121] If there are specific reasons for including those corporations on the list, the government should publicly state them in detail for each corporation before sanctioning them, so that the security risks are clear and there is no danger of the process becoming politicized. If they do not have a clear justification based on the listed criteria for inclusion, those corporations should be removed from the list.

Scrupulously upholding the rule of law is not just an ethical imperative if the U.S. government wishes to criticize China for its own alleged lawlessness. It also avoids providing further evidence that the U.S. is being hypocritical and unjustifiably singling China out for criticism.[122] And if too many Chinese corporations and entrepreneurs are arbitrarily included on various sanctions lists without clearly published justifications, in the longer term this is likely to lead to counter-sanctions that stifle U.S. corporations in China, harming U.S. economic development; and it will discourage highly talented Chinese individuals from contributing their skills to advanced technological innovation in the U.S., as they have in great numbers previously.[123]

More broadly, the contradictions revealed in Biden's list (and in the previous Trump lists) manifest deep-seated disagreements among various actors within the U.S. government about how to deal with a rising China. While currently, there appears to be bipartisan support for some types of sanctions against China, the extent of those sanctions and whether they should aim to suppress broader Chinese economic development on top of its military development are still hotly debated topics. Much of the debate seems to focus only on the perceived defects of the Chinese Communist Party (CCP) and its "threat" to the "international order," while overlooking the economic benefits that the CCP has brought to Chinese people and to its trading partners (including the U.S.). These benefits could not have been achieved without the admission of Chinese businesses into the relatively open international trading system over the past two decades.[124] The underlying assumption of the more hardline proponents of broad economic sanctions that a "decoupling" of the U.S. and its allies from China would somehow protect the national security of these nations is not supported by the history of modern China. During most of the Maoist period when China was largely cut off from international engagement, between 1949 and 1976, Chinese people were living in relative poverty and occasionally experienced deadly famines; and China's military

[121] Though we only identified 9 corporations whose inclusion on Biden's list is suspect, note that among the 59 entities, at least 10 are either parent or subsidiary corporations of others on the list, so the proportion of corporations whose inclusion is suspect is around 20%.

[122] *See*, for example, Xinhua, *supra* note 82.

[123] For this last point, *see* Brunner and Weinstein, *supra* note 38.

[124] The benefits to the U.S. of the trading relationship are reflected in the massive losses to U.S. firms projected by the U.S. Chamber of Commerce in various industry sectors adding up to hundreds of billions of dollars if decoupling were to occur: *see* U.S. CHAMBER OF COMMERCE, UNDERSTANDING U.S.-CHINA DECOUPLING 3–4 (2021).

conflicts with its neighbors (and with U.S. forces in the East Asian region, such as in South Korea) were much more widespread and serious than they have been since the 1980s.[125]

Clearly, if sanctions are to realize their purpose without unnecessarily harming ordinary Chinese citizens and civilian businesses, they must be very carefully targeted, with clear and consistent objectives, and backed up by meticulously collected and transparently published evidence that justifies imposing them on specific entities. They must also demonstrably protect U.S. national security more than the previous approach of active and positive engagement. The current Biden list and its implementation do not meet these basic criteria.

[125] For a useful overview of the Maoist period, see 14–15 THE CAMBRIDGE HISTORY OF CHINA (Roderick Macfarquhar & John K. Fairbank eds., 1991).

APPENDIX: TABLES OF CHINESE CORPORATIONS DIVIDED INTO RELEVANT CATEGORIES

TABLE 1: CORPORATIONS WITH CLEAR DEFENSE OR RELATED MATERIEL OPERATIONS

Corporation Name	**Industry Sector**	**Defense or Related Materiel Links**	**Source of Information**
Aviation Industry Corporation of China (AVIC)	Aviation sector	State-owned aerospace and defense conglomerate. It provides civilian and military aircraft production. Company products include fighter aircraft, transport aircraft, and helicopters.	*Introduction* Aviation Industry Corporation of China (2021), *available at* https://www.avic.com/c/2021-03-26/511215.shtml.
AVIC Aviation High-Technology Company Limited		A subsidiary of AVIC and a listed company on the Shanghai Stock Exchange. Main business activities include new material application and developing AI smart equipment	*Company profile*, AVIC Aviation High-Technology Company Limited(2021), *available at* http://www.avicht.cn/zh-cn/avicht.aboutus.
AVIC Heavy Machinery Company Limited		A large subsidiary of AVIC specializing in aviation forging and casting, hydraulic environment control, and other key defense aviation products.	*Introduction*, AVIC Heavy Machinery Company Limited(2021), *available at* http://www.hm.avic.com/gxwm/gcjg/index.shtml
AVIC Jonhon Optronic Technology Co., Ltd.		A subsidiary of AVIC and a listed company on the Shenzhen Stock Exchange. It hosts the largest Chinese lab on military electronics and it is the largest supplier of defense photoelectric connectors.	AVIC Jonhon Optronic Technology Limited, *Company profile*, Shenzhen Stock Exchange(2021), *available at* https://finance.ifeng.com/app/hq/st

			ock/sz002179/index.shtml.
AVIC Shenyang Aircraft Company Limited		A member of the AVIC group, the largest manufacturer of war aircraft and air fighters in China.	*About us*, AVIC Shenyang Aircraft Company Limited(2021), *available at* http://sfm.avic.com/gxwm/gcjg/index.shtml
AVIC Xi'an Aircraft Industry Group Company Ltd.		A member of the AVIC group with main products including large and medium-sized transport aircraft, bombers, special war aircraft, etc.	*About us*, AVIC Xi'an Aircraft Industry Group Company Ltd.(2021), *available at* https://www.xac.com.cn/gywm/gsjj/
Jiangxi Hongdu Aviation Industry Co., Ltd.		a member of the AVIC group. Hongdu has developed into a scientific research and production base for China's trainer aircraft, attack aircraft, and light general-purpose aircraft, as well as an aviation foreign trade export base.	*About Us*, Jiangxi Hongdu Aviation Industry Co., Ltd.(2021), *available at* https://web.archive.org/web/20120822232030/http://www.hongdu.com.cn/news/zjhd_s.asp?id=184
Zhonghang Electronic Measuring Instruments Company Limited		A company specializing in helicopter suspension systems, joystick control systems, and aircraft power distribution systems for defense use.	*Products and Services*, Zhonghang Electronic Measuring Instruments Company Limited. (2021), *available at* http://www.zemic.com.cn/products/list?cate=1
China	Aerospace	CASIC is a Chinese state-	CASIC, *About*

Aerospace Science and Industry Corporation Limited (CASIC)	Industry	owned enterprise that designs, develops and manufactures a range of spacecraft, launch vehicles, strategic and tactical missile systems, and ground equipment. CASIC is the largest maker of missiles in China.	*Us* (2021), *available at* http://www.casic.com.cn/n12377374/n12378092/index.html.
China Aerospace Science and Technology Corporation (CASTC)		CASTC is the main contractor for the Chinese space program, which designs, develops, and manufactures a range of spacecraft, launch vehicles, strategic and tactical missile systems, and ground equipment.	CASC, *About Us* (2022), *available at* http://www.spacechina.com/n25/n142/index.html.
China Aerospace Communications Holdings Group Company Limited (CAC Holding)		CASIC is the largest shareholder of CAC Holding, with 56.95% of the company's shares. The main business activities of CAC Holding include the production of Aerospace defense communication equipment and production of special vehicles.	CAC Holding, *Report on Investment Risk Analysis of Aerospace Communication Holding Group Co., Ltd.*, CAC Holding (2021), *available at* http://www.aerocom.cn/n3694005/n3694146/c21304669/content.html.
China Aerospace Times Electronics Co., Ltd (CATEC)		CATEC is the listed arm of CASTC, principally engaged in the research, development, and manufacture of aerospace electronics products to be used in launch vehicles and satellites.	CASTC, *Information disclosure of CATEC* (2022), *available at* http://www.spacechina.com/n25/n142/n162/n4623/index.html.

China Avionics Systems Company Limited (CASCL)		As a subsidiary of AVIC, CASCL is principally engaged in the manufacture and distribution of aviation and defense electronic products such as aircraft data acquisition equipment, autopilots, cockpit control and dimming systems, and sensor components.	CASCL, *About Us* (2021), *available at* http://www.aviconics.com.cn/gxwm/ldzc/index.shtml.
China Spacesat Co., Ltd.		China Spacesat Co., Ltd. engages in the operation of satellite applications, and the research, manufacturing, and system integration of satellite and satellite application products.	China Spacesat, *About Us* (2021), *available at* http://www.spacesat.com.cn/templates/content/index.aspx?nodeid=4.
Aerosun Corporation		Aerosun Corporation is a listed company under the AVIC Group, engaging in the research, design, and manufacture of civil nuclear waste disposal equipment, special vehicles including military trucks, and industrial piping.	Aerosun Corp., *Introduction* (2021), *available at* http://www.aerosun.cn/n3181391/index.html; and *Products and Services* (2022), http://www.aerosun.cn/n3379707/index.html
China Academy of Launch Vehicle Technology (CALT)		A civilian and military space launch vehicle manufacturer. It is a subsidiary of China Aerospace Science and Technology Corporation (CASC).	*Get to know us*, China Academy of Launch Vehicle Technology (2021), *available at* http://calt.spacechina.com/n481/n489/index.html
Aero Engine Corporation of China		Aero Engine focuses on the design and development of aero engines and related	*Introduction*, Aero Engine Corporation of

		technology. Aero Power Machine, a key company product, is used in military equipment.	China (2021), *available at* http://www.aecc.cn/jqgk/jqjg/index.shtml
Aerospace CH UAV Co., Ltd		A listed company specializing in developing unmanned aerial vehicles (UAV) and UAV airborne weapons.	*About us - HTCH*, Aerospace CH UAV Limited, *available at* http://www.htchuav.com/about.html#d1
Guizhou Space Appliance Co., Ltd (GSA)		GSA is a professional solution provider and manufacturer of relays, connectors, and cable assemblies. There are four plants in China and two R&D centers. Major products are produced for the aerospace industry. GSA is listed on the Shenzhen Stock Exchange.	GSA, *About Us* (2021), *available at* http://www.gzhtdq.com/about.
China Satellite Communications Co., Ltd. (China Satcom)		China Satcom is a main subsidiary of CASC specializing in satellite communications and broadcasting services.	China Satcom, *About Us* (2021), *available at* http://www.csat.spacechina.com/n782699/n782739/index.html.
North Navigation Control Technology Co., Ltd. (Norinco Group)		Norinco Group is principally engaged in the manufacture and sale of military and civilian products. Its civilian products mainly include special vehicles and other high-tech products.	Norinco Group, *Company Introduction* (2021), *available at* http://bfdh.norincogroup.com.cn/col/col1027/index.html.
Shaanxi Zhongtian		As a subsidiary of CACTC, Zhongtian Rocket	CACTC, *Zhongtian Rocket*

Rocket Technology Company Limited (Zhongtian Rocket)		manufactures and distributes defense products such as small solid rockets, nuclear-guided missiles, and aircraft broadcast systems, as well as civilian products such as forest fire fighting bombs, weather radars, and other related products.	(2021), *available at* http://www.spacechina.com/n25/n142/n162/n3018970/index.html.
Anhui Greatwall Military Industry Company Limited	Military Supplies & Vehicles	A listed company that manufactures and supplies war-related products, clearly identified by its name.	Anhui Great Wall Military Industry Company Limited, *Key business, and services* (2021), *available at* http://www.ahccjg.com.cn/
China North Industries Group Corporation (Norinco Group)		Manufactures a wide range of civil and military defense products. This company is also involved in domestic civil and military construction.	*About Us*, China North Industries Group Corporation (2021), *available at* http://www.norincogroup.com.cn/col/col12/index.html
China South Industries Group Corporation		A central government company that manufactures automobiles, motorcycles, firearms, vehicle components, electronic products, and other special products domestically and internationally, for civilian and military use.	*Introduction* China South Industries Group Corporation (2021), *available at* https://www.csgc.com.cn/col/24578
Inner Mongolia First Machinery Group Co.,		This is a subsidiary of Norinco Group located in Inner Mongolia. This company floated its subsidiary on the Shanghai	*About Us*, Inner Mongolia First Machinery Group Ltd (2021), *available*

Ltd		Stock Exchange in 2016. Its main business is to manufacture war supplies for the PRC army, air force, and navy.	*at* http://yjjt.norincogroup.com.cn/col/col1076/index.html
China National Nuclear Corporation	Nuclear Industry	A State-owned corporation that is committed to developing China's civilian and military nuclear programs. CNNC has set up a nationwide industrial conglomerate integrating science, technology, industry, and international trade.	*Development in the past 5 years*, China National Nuclear Corporation (2021), *available at* https://www.cnnc.com.cn/cnnc/xwzx65/zhyw0/1135276/index.html
China Nuclear Engineering Corporation Limited		This company is a main part of the PRC's national nuclear technology industry and a leading entity in developing China's national strategic nuclear forces and nuclear energy.	*Introduction*, China Nuclear Engineering Corporation Limited (2021), *available at* https://www.cnecc.com/1802.html
CSSC Offshore & Marine Engineering (Group) Company Limited (CSSC offshore)	Shipbuilding and Maritime Industry	CSSC Offshore produces and manufactures comprehensive marine and defense equipment including military ships, marine police equipment, industrial Internet platforms, and other related defense products.	CSSC offshore, *Company Introduction* (2021), *available at* http://comec.cssc.net.cn/.
China State Shipbuilding Corporation Limited (CSSC)		CSSC manufactures and sells ships. The Company produces oil tankers, bulk carriers, conditioner vessels, deepwater survey ships, and marine equipment.	CSSC, *About Us - our company* (2021), *available at* http://www.cssc.net.cn/n4/n12/index.html.
China Shipbuilding		CSICL operates as a ship manufacturer for products	CSIC, *About Us* (2021), *available*

Industry Company Limited (CSICL)		including naval ships, warship diesel engines, shipborne weapon launchers, navigation equipment, communication equipment, and other military warship equipment.	*at* http://www.csicl.com.cn/n327/n328/index.html.
China Shipbuilding Industry Group Power Company Limited (CSICP)		CSICP designs, produces, and markets naval and maritime power systems including electricity, gas, steam, chemical, diesel, civil-nuclear, and stirling engines.	CSICP, *Company Introduction* (2021), *available at* http://www.china-csicpower.com.cn/n373/n374/index.html.
China Marine Information Electronics Company Limited (CMIE)		CMIE develops, produces, and distributes underwater information transmission equipment, underwater weapons system special equipment, marine special power supply products, and other defense products.	CMIE, *About the company* (2021), *available at* http://www.cmie.csic.com.cn/n405/n411/index.html.
Changsha Jingjia Microelectronics Company Limited (Jingjia)	Defense electronics sector	Jingjia manufactures defense-related supplies and equipment including radar, missiles, launch vehicles, and military microwave electronics. Jingjia is the largest Chinese defense supplier of microwave electronics and defense chips.	Changsha Jingjia Microelectronics Company Limited (2021), *Quarterly report*, *available at* https://xinpi.stcn.com/finalpage/2021-10/29/1211419160.PDF
China Electronics Corporation (CEC)		CEC manufactures military products including midstream system-level products, mainly for aircraft and ships, and downstream complete machine products, such as air defense and air	China Electronics Corporation (CEC), *About the company* (2021), *available at* https://m.cec.co

		traffic radar systems.	m.cn/jtjj/list/index_1.html; and Chao Zhang, et al., *Six important questions about defense industry*, AVIC security institute (2021), *available at* https://pdf.dfcfw.com/pdf/H3_AP202101081448976148_1.pdf?1610141482000.pdf.
China Electronics Technology Group Corporation (CETC)		A Chinese state-owned company. Its fields include communications equipment, computers, electronic equipment, software development, research services, investment, and asset management for civilian and military applications.	*Introduction and Group Leader - CETC* China Electronics Technology Group Corporation (2021), *available at* https://web.archive.org/web/20160915075940/http://en.cetc.com.cn/enzgdzkj/about_us/introduction29/index.html.
Costar Group Co., Ltd		Costar is a wholly state-owned company affiliated to China North Industries Group Corporation, a large-scale enterprise in the national optoelectronic industry, and a national export base enterprise for electromechanical products.	*Company Profile*, Zhongguang Limited CoStar (2021), *available at* https://www.csgc.com.cn/hn508/default.aspx
Fujian Torch Electron Technology Co., Ltd		The company's products are widely used in aviation, aerospace, shipbuilding, communications, electric	Fujian Torch Electron Technology Limited,

		power, rail transit, new energy, and other fields. Defense-related products and services are the key revenue source for this company.	*Founded in 1989 - introduction of the company* (2021), *available at* https://www.torch.cn/about.php?nav=15; Fujian Torch Electron Technology Company Limited, *Prospectus for Fujian Torch Electron Technology Company Limited*, China Securities Regulation Commission (2014), *available at* http://www.csrc.gov.cn/zjhpublic/G00306202/201410/P020141022556318280944.pdf
Inspur Group		Inspur is China's largest server manufacturer and provider with products widely used in various defense sectors such as land, sea, air, and armed police, as well as 10 major military industry corporate groups including China Power, China Shipbuilding and Aerospace, etc.	Inspur Group, *About Inspur Group* (2021), *available at* https://www.inspur.com/lcjtww/gylc32/2315125/index.html
Nanjing Panda Electronics Company		Nanjing Panda is a subsidiary of Panda Electronics Group Co., Ltd. (Panda Group). The	Panda Electronics Group, *About Nanjing Panda*

Limited (Nanjing Panda)		company develops, manufactures, and markets mobile telecommunications, satellite communication, information technology, and electromechanical products.	*Electronics Company Limited* (2021), *available at* https://www.panda.cn/gsjj/index_19.aspx.
Panda Electronics Group Co., Ltd. (Panda Group)		Panda Group is a leading supplier of intelligent manufacturing under China Electronics (CEC) and the largest central enterprise in the electronics industry and a large PRC defense conglomerate. Its products include industrial robots, and intelligent manufacturing systems and intelligent manufacturing solutions in China's national defense electronic countermeasures industry.	Panda Electronics Group Co., Ltd., *About Us - who are we, what are we doing and future goals* (2021), *available at* http://www.panda-fa.com/intro

TABLE 2: GROUP 1 CORPORATIONS WITHOUT CLEAR DEFENSE OR RELATED MATERIEL LINKS

Corporation name	**Industry sector**
China Railway Construction Corporation Limited (CRCC)	Construction/Infrastructure
China Communications Construction Company Limited (CCCCL)	
China National Offshore Oil Corporation (CNOOC)	Resources (oil and gas)
China Telecommunications Corporation (China Telecom)	Telecom/internet services
China United Network Communications Group Co., Ltd (China Unicom)	
China Mobile Communications Group Co., Ltd. (China Mobile)	
Semiconductor Manufacturing International Corporation	Technology manufacturing

(SMIC)	
Hangzhou Hikvision Digital Technology Co., Ltd. (Hikvision)	Audio/video technology
Huawei Technologies Co., Ltd. (Huawei)	Telecom/network equipment

TABLE 3: CORPORATIONS THAT OWN/CONTROL OR ARE OWNED/CONTROLLED BY OTHERS ON THE LIST

Group 3 Corporation	**Relation to Group 1 or 2 Corporation**
China Communications Construction Group (Limited)	Subsidiary of China Communications Construction Company Limited
China Electronics Corporation	Subsidiary of China Electronics Technology Group Corporation
China Mobile Limited	Subsidiary of China Mobile Communications Group Co., Ltd.
China Telecom Corporation Limited	Subsidiary of China Telecommunications Corporation
China Unicom (Hong Kong) Limited	Subsidiary of China United Network Communications Group Co., Ltd.
CNOOC Limited	Subsidiary of China National Offshore Oil Corporation
Huawei Investment & Holding Co., Ltd.	Parent of Huawei Technologies Co., Ltd.
Proven Glory Capital Limited[126]	Subsidiaries of Huawei Technologies Co., Ltd.
Proven Honour Capital Limited	
Panda Electronics Group Co., Ltd[127]	Parent of Nanjing Panda Electronics Company Limited

[126] Jose Ye, *US-China Tech War: Biden Cuts Two Huawei Financing Arms Off From US Investor Access as Fight Moves To Capital Markets*, S. CHINA MORNING POST (Jun. 4, 2021).

[127] Panda Electronics Group Co., Ltd, actually appears twice on the list of three groups (in groups 1 and 3), which must be an error, as a single company cannot control itself: see White House, "Fact Sheet." However, we assume that the correct category is Group 3, as the subsidiary Nanjing Panda Electronics Company Limited appears only in Group 1.