

The Science, Indigenous Technology and Advanced Research Accelerator

**To**

**Dr Rajesh Pant**

**National Cybersecurity Coordinator**

**NSCS**

May 11, 2021

**CLP Group HK acquiring strategic North Eastern power transmission line**

Dear Dr Pant,

Kindly permit us to draw your kind attention to the media report regarding Govt seeking ownership details from the “***Hong Kong-based***CLP Group, before allowing its unit CLP India Pvt. Ltd to ***acquire an important power transmission link in the strategic North-East region*”** (<https://www.livemint.com/industry/infrastructure/govt-seeks-response-from-clp-on-ownership-details-11609953384717.html>). CLP India Private Limited is seeking to acquire shares in the Kohima Mariani Transmission Ltd. from an Indian company - Kalpataru Power Transmission Limited (KPTL) and Techno Electric and Engineering Company Limited. Articles which show that KPTL is a highly successful private sector Indian MNC are enclosed.

We commend the Govt for looking more closely at ownership details of a company headquartered in Hong Kong, CLP Holding. Hong Kong has recently lost all semblance of autonomy following a brutal crackdown by China and by its proxies in the HK Govt: **for all practical purposes, so far as India’s national defence is concerned - Hong Kong is China. We do not expect KPTL to keep national security/ national interest in mind but Government must look at the national and economic security consequences of this potentially dangerous deal:**

1. This transmission line runs through **3 sensitive border States beyond the chicken’s neck** --**Manipur, Nagaland and Assam**. **It should be immediately apparent why a Hong Kong / China based company seeks control over it.** Moreover, the transmission lines consist of equipment including **smart components, Supervisory Control and Data Acquisition (SCADA) systems, control and protection devices, and remotely controlled assets. It is essential that national control over data, communications and supervision is retained, which is why world-wide the power sector is considered sensitive and critical infrastructure.**
2. **China has designs on our water resources in the North East region and is constructing dams in its territory to control and manipulate** **the flow of water to Indian river systems. To give it control over such a strategic border asset goes against every tenet of National Security**.
3. **The ownership of the company is carefully disguised,** with headquarters varyingly shown as India/ Mauritius/ Hong Kong. Be that as it may, there is no doubt that **HK/ China based companies have to follow Beijing’s orders. No company headquartered in Hong Kong is safe from Chinese control. Even Chinese companies owned by Pres. Xi's rivals are shifting base to Singapore** (WSJ article enclosed). **Pres. Xi felled even the mighty Ant's IPO because his political rivals had reportedly taken sizable stakes in Ant.** **Giving security clearance just because the Board of Directors of CLP Holdings is white-skinned with a fair sprinkling of Chinese / HK nationals, would be short-sighted and detrimental to National Security.**
4. **As mentioned, the power sector is rightly classified in most countries as a critical infrastructure sector and rightly so designated by Ministry of Power (MoP) as sensitive and critical, more so as with the introduction of smart grids and other remotely operable digitised equipment, it has become vulnerable to cyberattack, as the recent massive Mumbai power outage (which is only a trailer, with many more to come) following the Galwan murders of Indian soldiers showed.**
5. **As a rule, every foreign investment proposal in the power sector should be scrutinised for potential National Security risks. SITARA has repeatedly pointed out the need to protect our power grids and ICT infrastructure against foreign penetration and potential subversion (**<https://sitara.org.in/editorial/chinese-cyber-attack/>). **We had written to the Minister for Power** (letter enclosed) **commending him for the recent decision to halt imports of Chinese equipment in the power sector and pointing out how agencies flouted Hon’ble Prime Minister’s directives on Atmanirbharta - in the power sector before and even after the Galwan attacks.**

**A CFIUS like body for India**

1. **This underlines the need to take a more strategic, National Security perspective on Foreign Direct Investment (FDI) proposals, which is why we are writing to you – an agency entrusted with India’s National Security. The fashion of selling off our best firms without any long-term vision on security, dividend & profit repatriation, is flawed and contrary to National Interest. We need to take into account:**
2. **National Security implications, whether the acquisition gives undue control to a foreign entity over critical strategic assets and resources** (such as power, pharmaceuticals, communications and cyber networks, financial sector, defence industrial base, nuclear, transportation – list of US CI sectors attached as an example).
3. **The case under consideration is a brownfield acquisition and does not create additional capacity nor does it generate additional employment. Instead, a valuable Indian company operating critical infrastructure in sensitive border areas will pass under Chinese control.**
4. **The foreign exchange gained will be a one off, but the security consequences will stay.**
5. **India must promote its own companies and not sacrifice long-term national and economic security interest especially to one-time, brownfield FDI. It is in India's interest to create powerful domestic champions. KPTL is doing very well, and any partnership with HK/Chinese firms especially in border areas must be looked upon with EXTREME suspicion. In the instant case KPTL seems to wish to divest its shares. Let another Indian owned private sector/ PSU step up and buy them. Ownership of these strategic assets must stay in Indian hands. We need to learn lessons from the Mumbai Powergrid hack. We have already alienated a lot of our power infrastructure to China. We must stop this.**
6. **Moreover, profits outflows etc will be in perpetuity. This is why countries with more foreign assets abroad (most developed countries) have a National Income greater than GDP, while the National Income of developing countries like India which host FDI is lower than our GDP because of the constant outflow of profits from FDI and other assets held by foreigners.**

**We would like to draw your attention to Prof Dhar/ Prof Chalapathi Rao’s masterful analysis of FDI inflows into India which shows that very little useful, greenfield manufacturing FDI has actually flown in, in the recent period under study** (Prof Dhar & Prof K.S. Chalapati Rao’s ISID essay “Assessing India’s Inward FDI”, http://isid.org.in/indias-recent-inward-foreign-direct-investments-an-assessment)**.**

**(Disclaimer: We are fully in favour of greenfield, high-tech manufacturing FDI).**

**Conclusion**

* **It would be utter folly to alienate shares in one of India’s most successful companies and hand them over to a Hong Kong based company subject to Chinese jurisdiction.**
* **This Govt is committed to National Security. This transfer/ acquisition goes against the basic tenets of National Security and thus must be blocked.**
* **We are annexing a proposal to create an Indian equivalent of the Committee on Foreign Investment of the United States** (CFIUS: an interagency committee authorized to review foreign investments/ real estate transactions by foreign persons, in order to determine the effect of such transactions on national security.)

With best regards and best wishes for your and your team’s safety,

(Smita Purushottam)

Chairperson SITARA

Annex

**Annex**

**Need for a Committee on Foreign Investment in India patterned on the CFIUS**

India needs a mechanism for monitoring and if necessary, rejecting foreign investments which harm its national security and economic foundations. It can therefore draw lessons from the American experience on blocking and controlling Chinese FDI.

2. China has been snapping up high-tech US (and European) companies in a range of critical sectors as part of its advanced technology acquisitions strategy. Despite the existence of the Committee on Foreign Investment in the United States (CFIUS) established in 1975, many valuable technology companies have been acquired by China. China has also successfully exploited loopholes in CFIUS, focusing for example on start-tech ups which fall below the threshold for investigation.

3. So aggressive has been China’s acquisitions drive, that US Presidential Orders have been used to block/ reverse Chinese acquisitions of high-tech companies like Lattice Semiconductor (2017); Xcerra, maker of equipment to test computer chips and circuit boards; Aixtron, a German semiconductor company’s US subsidiary (2016), and Mamco, an aeroplane parts manufacturer (1990). Acquisitions of High-tech Aerospace companies - Boeing, Airbus-EADS, Honeywell, Embraer, Safran, GE etc - have complemented Forced Technology transfers in exchange for FDI in China. By 2016, Chinese cumulative Overseas Direct Investment (ODI) in the US reached US$ 45 bn, while globally, Chinese ODI shot up to $196 bn. The takeover of high-tech American and European companies significantly bolstered China’s technological and military capabilities and its capacity to do mischief.

4. China’s rise as a technological and geopolitical challenge has prompted the US to take more decisive measures to block China’s access to advanced US technologies. The United States has adopted the Foreign Investment Risk Review Modernization Act (FIRRMA) as part of the National Defense Authorization Act (NDAA) 2019 in August 2018 (texts enclosed). FIRRMA strengthens the powers and scope of CFIUS as follows:

* **Mandates and strengthens CFIUS to apply more extensive national security considerations while checking foreign investments**, thus firmly providing national security oversight over foreign investment.
* **Expands the areas under CFIUS jurisdiction**, mandating it to pay attention to the national security impact of foreign control of critical infrastructure, energy assets, critical materials, critical technology and many other new areas.
* **Closes loopholes to prevent Chinese companies** entering into investment partnerships designed to avoid CFIUS reviews or exercising control over decision-making in strategic companies even with a minority presence.
* **Emphasises the need to maintain superior military and technological capabilities with “potential peer and near peer military or economic competitors”.**
* **Refers to “a country of special concern**” with “a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security.” It also refers to countries “that may pose a **significant threat to the national security of the United States”.**
* Steps up export controls as these are required to preserve the qualitative military superiority of the United States and strengthen the United States defense industrial base. FIRRMA baldly declares that export controls should ensure “**that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation” – which the national security of the United States requires.**
* **Provides for very detailed biennial reports of Chinese investments in the US by type, sector, amount etc.**

**5. Impact**: Recent figures show that there has been a steep fall in Chinese ODI in the US, which is now “projected to fall from $29.4 billion in 2017 to $4.0 billion”.

**National Security includes technological and economic superiority**

6. Clearly, the US definition of national security encompasses economic and technological superiority over “countries of concern” (directed mainly at China). In fact, **in FIRRMA**, a legislation dealing with *investment risks*, the term **‘National Security’ appears 82 times** and the text goes into great detail over many more aspects of the National Security risks posed by foreign investments by adversaries and countries of concern. It should be required reading by policy makers in India in charge of defence, economic and technology policies.

**National Defense Authorization Act (NDAA) 2019**

7. Not just FIRRMA, but also the NDAA 2019 of which it is a part, should in fact be analysed in full by our National Security agencies. It is a comprehensive playbook on how to shore up National Security in the technological and economic spheres and sharpen American capabilities to meet the China threat, underlining how seriously the Americans take the latter and how far China has reached, which has security implications for India. Some (but by no means exhaustive) examples of the references in the NDAA to maintaining the US’ technological edge in cutting edge, frontier areas are provided below. The US Govt has taken several measures pursuant to the NDAA’s directions.

* **Banned US Government procurement / extension of contracts for telecommunications / surveillance equipment from China**, specifically identifying but not restricted to Huawei, ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company and Dahua Technology Company. It also prioritised government assistance to affected American entities for transitioning from Chinese equipment and services.
* **Enjoined on the Secretary of Defense to publish annual ``National Defense Science and Technology Strategies''** which will include technology priorities, goals, and investments. The Secretary would also need to prepare *comparisons with the enterprises of other countries*.
* Directed the Secretary of Defense to carry out **a quantum science and technology R&D program to ensure global superiority of the United States** in quantum information science necessary for meeting national security requirements.
* Directed the Secretary of Defense to ensure coordination to develop, mature, and transition **Artificial Intelligence technologies** into operational use.
* Directed the Secretary of Defense, with the Director of the Defense Intelligence Agency, to submit classified reports comparing the capabilities of the United States in emerging technology areas with those of its adversaries - in: (1) Hypersonics. (2) Artificial intelligence. (3) Quantum information science. (4) Directed energy weapons. (5) other emerging technical areas.
* **Required a report containing a whole-of-government strategy** with respect to the following activities by the CCP, as the NDAA declared that “long-term strategic competition with China is a principal priority for the United States that requires the integration of multiple elements of national power, including diplomatic, economic, intelligence, law enforcement, and military elements, to protect and strengthen National Security”:

“(i) The use of political influence, information operations, censorship, and propaganda to undermine democratic institutions and processes, and the freedoms of speech, expression, press, and academic thought.

(ii) The use of intelligence networks to exploit open research and development.

(iii) The use of economic tools, including market access and investment to gain access to sensitive United States industries.

(iv) Malicious cyber activities.

(v) The use of investment, infrastructure, and development projects, such as China's Belt and Road Initiative, in Africa, Europe, Central Asia, South America, and the Indo-Pacific region, and the Polar Silk Road in the Arctic, as a means to gain access and influence.

(vi) The use of military activities, capabilities, and defense installations, and hybrid warfare methods, short of traditional armed conflict, against the United States or its allies and partners.

(B) Available or planned methods to enhance strategic communication to counter Chinese influence and promote United States interests.

(C) An identification of the key diplomatic, development, intelligence, military, and economic resources necessary to implement the strategy.

(D) A plan to maximize the coordination and effectiveness of such resources to counter the threats posed by the activities described in subparagraph (A).

(E) Available or planned interagency mechanisms for the coordination and implementation of the strategy.”

* **Demanded a report on the military and coercive activities of China in the South China Sea.**

8. **Of potential interest to India is the proviso in the FIRRMA text for the US President to conduct a more robust international effort to help allies and partners to establish processes similar to CFIUS to screen foreign investments for national security risks - and to facilitate coordination. This could open the path to collaboration on this issue with the US or even inclusion in the Exemption list of countries from which the US does not seek FDI reviews if we have sound National Security legislation to protect our companies from takeovers by hostile powers. As per a media report, Michael McCaul, US House Foreign Affairs Committee Republican, and China Task Force Chairman, has praised India's decision to exclude Chinese "Communist Party-controlled" companies from participating in 5G.**

**The EU follows America’s lead on National Security review of FDI**

9. The EU has adopted an **FDI Regulation (**11 October 2020) establishing “a framework for the screening by Member States of FDI” ***on security grounds***, with a mechanism for cooperation, in the wake of an outcry in Germany, France and Italy regarding Chinese takeovers of high-tech companies, including that of the advanced robotics German company Kuka. Thus, high-tech Germany was the most targeted country for Chinese ODI, and Germany cancelled Chinas’ acquisition of Aixtron, a semiconductor equipment manufacturing company. The areas covered in the EU regulation and concerns are similar to the US: critical infrastructure; sensitive facilities; land and real estate crucial for the use of such infrastructure;

 critical technologies and dual use items;

supply of critical inputs;

access to or the ability to control sensitive information, including personal data; and

media freedoms. Also, it is directed at China in that it enjoins Member States and the Commission to consider “whether the **foreign investor is directly or indirectly controlled by the government, including state bodies or armed forces, of a third country”.**

**10.** Several EU member countries (and others) have joined the US Clean Network Initiative, which seeks to **remove Chinese telecom companies from national and international Communications Networks, and have banned Chinese companies from participating in 5G rollouts.**

**China is not only cybersecurity threat**

11. However, security concerns are not all directed at China. Thus, the UK Government intervened in an **American** company (Nvidia) buying out a company in the UK (Arm) **on grounds of National Security** (<https://www.bbc.co.uk/news/business-56804007>). **Chip making is as sensitive as it gets.**

12. **The UK could have done this more circumspectly, by placing tax and other hindrances in the way of the acquisition, instead they chose to advertise their National Security concerns with a US acquisition in public.**

**13. We have been pointing out that the only way to secure India’s cyber infrastructure is to fully indigenise both the networks and the cybersecurity solutions. Utmost vigilance on national security grounds in clearing FDI and in procurement decisions for these sectors is required.**

**Economic argument for carefully reviewing FDI in India**

14. Finally, there is an economic argument for carefully reviewing FDI in India, quite apart from security considerations relating to Chinese investment. Economic security is National Security. Uncontrolled FDI does not benefit India. There is no automaticity of benefits accruing to India from FDI (Prof Dhar & Prof K.S. Chalapati Rao’s ISID essay “Assessing India’s Inward FDI”, http://isid.org.in/indias-recent-inward-foreign-direct-investments-an-assessment). Most FDI is flowing into services and Brownfield sectors **and valuable Indian companies are passing into foreign hands**. Moreover, reverse repatriations and divestments are quite sizable. So-called investment in R&D Centres brings little benefit to India as the IP and designs are all held by foreigners. **All this means that in the medium to long-term, outflows will accelerate and reduce National Income. The National Income of developed countries is higher than their GDP, and the reverse is true for India which sees a substantial outflow of proceeds on account of assets held by foreigners in India. Unless FDI is directed to high-tech, greenfield manufacturing activities, India will see little benefit in terms of capacity creation, managerial upgrades and employment and skills generation.**

**CONCLUSIONS AND RECOMMENDATIONS**

1. **The US FIRRMA/ NDAA clearly amounts to a very intrusive and strong Industrial Policy. We request our National Security agencies to treat the neoliberal advice emanating from some agencies with great caution – it is clear that while developed countries have pursued policies in their national interest, developing countries like India have been sold the opposite mantra – to discard Industrial Policy and not carefully scrutinise which investments are truly in the national interest/ benefit the economy in a substantive manner. We shall analyse different elements of US Industrial Policy in separate notes, but the most advanced nation in the world has been practising Industrial Policy over decades even as its neoliberal elites preach to us about its irrelevance. India should make up its own mind what is good for its long-term National Security and Economic Security and adopt legislation/ take action accordingly. As we said long ago – “copycats don’t catch mice” (this is a take from Deng Xiaoping’s famous dictum about the irrelevance of the color of the cat etc.)**
2. A structure similar to CFIUS is highly overdue in India. It is very important to analyse the ownership structures / national security risks / overall economic benefits of companies investing in India, as the case in question refers. The free pass that we have given to FDI is damaging both National Security and economic security. A thorough review of FDI should be initiated by National Security Agencies and a comprehensive analysis of its impact/ benefits should be conducted. At the very least, a mechanism should be immediately created to monitor the National Security risks of some FDI and devise guidelines and an inter-agency mechanism for reviewing and monitoring it.
3. **While CFIUS is chaired by the Secretary of the Treasury, given India’s different circumstances, we strongly recommend the FDI review inter-agency committee have a strong security/ defence lead. At the very least, the NSCS should provide the Secretariat for the Committee.**

SITARA

Annex 2

**CFIUS COMMITTEE COMPOSITION**

The Secretary of the Treasury is the Chairperson of CFIUS

The members of CFIUS include the heads of the following

Department of the Treasury (chair)

Department of Justice

Department of Homeland Security

Department of Commerce

Department of Defense

Department of State

Department of Energy

Office of the U.S. Trade Representative

Office of Science & Technology Policy

The following White House offices also observe and, as appropriate, participate in CFIUS’s activities:

Office of Management & Budget

Council of Economic Advisors

National Security Council

National Economic Council

Homeland Security Council

The Director of National Intelligence and the Secretary of Labor are non-voting, ex-officio members of CFIUS with roles as defined by statute and regulation.