**EUROPE INDIA CHAMBER OF COMMERCE**
69, Boulevard Louis Mettewie (bte.18)
1080 Brussels (Belgium)
Tel & Fax: 0032 2 469 2677, 02-840 2800 GSM: 0472 207 338
E-mail: info@europeindia.eu; sunil.prasad@telenet.be Website: www.europeindia.eu
**Chairman: Ravi K Mehrotra, CBE Secretary General: Sunil Prasad**

EICC-2023 Brussels, 7 November 2023

Mr. Josep Borrell
EU High Representative for Foreign Affairs and Security Policy and
Vice-President of the European Commission
Brussels

Dear High Representative, Vice-President Mr. Borrell,

Re: **China's "magic weapon" and Challenge for Brussels**

On behalf of the Europe India Chamber of Commerce, the Apex Chamber of Brussels which acts as voice of industry on EU-India affairs, I am writing to you to draw your urgent attention to an issue which is serious in nature and has bearings on European Union's internal and external security including its democratic institutions.

I would particularly like to draw your attention to the shadow army of China's Communist rulers and its extensive spying machinery at work within the European Union that seems to have infiltrated various spheres of society, business and even institutions across Europe.

You must be aware that last month, Britain's domestic intelligence agency, MI5, warned of a "sharp rise in aggressive attempts" by China to steal Britain's technology secrets. It is not a secret that China and Russia have each sought to steal commercially sensitive data and intellectual property, as well as to interfere in domestic politics and sow disinformation in Europe. We fear that Chinese spying activities may be trying to infiltrate deeper into European institutions and policy making bodies in many Member States. As crucial elections to the European Parliament will take place in the next eight months, it is important that Brussels keep its guard up.

Not many know that Beijing's United Front Work Department (UFWD) is the shadow army of China's Communist rulers. The activities of UFWD pose a serious threat to democracies all over the world including EU. The prominence of the UFWD has witnessed a remarkable surge under President Xi Jinping. A frequently observed instrument of UFWD is the deployment of Chinese students studying in international universities. Chinese President has referred to United Front's work as a "magic weapon" crucial for realising the great rejuvenation of the Chinese nation, but in our view, it is a "deadly weapon" aimed at damaging and destroying Western democracy and its values. You are aware that President Xi has identified Western political values and institutions as the principal ideological threat to China.

The UFWD's activities in Brussels and in various capitals of EU countries canters on funding some think tanks and NGOs and influencing journalists and key figures within the strategic community. It has been noticed that many Chinese journalists based in Brussels have

been closely collaborating with UFWD. China's operations in Brussels extend beyond scholars and journalists; they encompass the active engagement of some former officials of EU institutions. It is therefore important that EU counters China's act, policies, practices and operations through strategic measures.

But these activities have not begun recently. They have been on for the past several years. You may recall that in a letter addressed to you on October 5, 2020, we had warned about the upsurge of Chinese espionage activities in Brussels. In the same year, two investigative journalists had uncovered the existence of an extensive network of Chinese intelligence agents in Brussels. As you know, in March the Belgian intelligence agency had placed Huawei on its watchlist and many of its senior lobbyists in Brussels under microscope for fears of Chinese espionage growing around the EU and NATO headquarters in Brussels.

Even you, Mr Borell, had raised the issue of malicious Chinese activities within the EU, in a statement on July 19, 2021. "*We have also detected malicious cyber activities with significant effects that targeted government institutions and political organisations in the EU and member states, as well as key European industries*" you had said and had urged Chinese authorities to take action against malicious cyber activities being undertaken from their territory.

But it seems that those warnings and pleas have had little effect. For, recently, Germany's domestic intelligence agency said that Beijing is clandestinely seeking to make Western politics more China-friendly by working on enlisting seasoned politicians.

The EU should also be concerned about the expansion of China's Counter-Espionage Law that took effect in July this year which bans the transfer of information it sees as related to national security. This should alarm the EU companies in China which could be punished for regular business activities. The EU businesses themselves need to be wary of the risk from Chinese authorities.

China's new Counter-Espionage Law is like a sword hanging on the heads of business executives functioning in the country. Because of this law, foreign employees in the country have been facing a serious risk since Beijing began tightening state control over information transfer related to national security and expanding the national security definition.

Previously, the legal definition of espionage focused on the disclosure of so-called state secrets and intelligence. The new version has expanded the definition to include documents, data, information, and items related to national security, as well as instigating, inducing, coercing, or bribing state employees.

A broader definition of national security allows Beijing "to detain and prosecute foreign nationals for alleged espionage". China uses exit bans to force foreigners to participate in government probes, to pressure the family members of dissidents overseas, and to gain leverage over foreign governments. The arrest in mid-October of a Japanese executive at Japanese drugmaker Astellas, detained since March on suspicion of "engaging in espionage activities and violating anti-espionage law," should serve as a wake-up call for European executives in China.

Sir, you will agree that China's behaviour reflects very poorly on China's ambition to become a great power and of its claim to play a leading role in global architecture. It is a

country that has contributed to creation of a global security crisis and a crisis of confidence, with its predatory activities and practises. You will also agree when we say that the greatest danger that West faces whether we are moving towards a world where China will be a norm setter, where countries will look at the Chinese successes and believe that they do not need to follow liberal democratic ideas and values. Therefore, EU cannot afford to underestimate and ignore any longer the immense and imminent danger that China poses to its institutions in particular and the entire society in general.

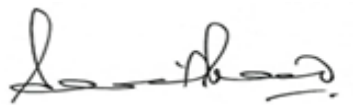
In the light of the above, we call upon you to review all options to firmly respond to, and deter, the PRC's espionage activities that threaten European Union's freedom, its values, its national security, and interests of its member states. As Beijing continues to test EU's resolve and tarnish its credibility, EU must respond with strength, or risk further aggression from its adversaries.

Thank you for your attention to this timely matter. We look forward to your reply.

On behalf of the entire EICC community, I would also like to extend to you the best wishes for the upcoming Holiday Season. May this Festive Season, which has already begun in India, bring happiness and peace to all.

With kind regards,

Yours sincerely,



Secretary General