



EUROHub4SINO

European Hub
for Contemporary China

August 2024

China's Sharp Power in the Western Balkans: Digital Technology as Asymmetrical Threat

by Paolo Pizzolo



Funded by
the European Union

POLICY RECOMMENDATIONS

Chinese sharp power-based disinformation and malign cyberactivity in the WBs aimed at spreading an anti-Western narrative is partly succeeding in slowing down EU regional integration and Euro-Atlantic enlargement, while increasing Beijing's commercial, strategic, and diplomatic assets, and introducing an alternative political-economic model to the West that pivots on the "Beijing consensus". In the coming years Beijing's ability to use technologies in order to undermine public trust in democratic institutions and the "clash of narratives" between China and the EU will find fertile ground in the WB6, where idiosyncratic political-economic visions will confront for regional hegemony.

Indeed, China's influence in the WBs, along with that of other non-EU actors such as Russia and Turkey, may *hinder* democratisation and Euro-Atlantic integration. In contrast to the EU and NATO, which place democratic conditions at the centre of their engagements with the Balkans, new outside players are less concerned with democracy, human rights, and the rule of law, focusing instead on trade opportunities, security assistance, and energy contracts. In addition, external autocratic actors have provided alternative sources of political and economic support to authoritarian and corrupt Balkan elites.

To adequately challenge these threats, the EU must:

-  Overcome its credibility crisis in the WBs, caused by years of enlargement fatigue within the EU.
-  Reverse the slow pace of reforms in the WB6 and reactivate the Berlin Process.
-  Advocate for a steady and rapid EU membership for the WB6.
-  Fortify the EU's geopolitical role in the region and outperform regional influences originating from the outside.

Keywords

Western Balkans

Sharp Power

Regional
Integration

Disinformation

Propaganda



Introduction

Over the past decade, non-Western external actors, including China, Russia, and Turkey, have gained increasing influence in the Western Balkans (WBs). Regarding China, its influence has been consolidating in the region, including through the framework of the 16+1 initiative and as part of the Belt and Road Initiative (BRI). As a result of geostrategic competition, the WB region has seen a persistent increase in Chinese influence that has allowed it to intensify its messaging on topics such as technological rivalry, pandemic management, vaccine diplomacy, governance systems, and geopolitical dilemmas. To gain political-cultural attractiveness, Beijing has promoted a soft power strategy akin to sharp power that, focusing on digital technology, relies heavily on propaganda and disinformation. In this sense, Beijing has actively exploited technology and technological devices to support disinformation campaigns. Empirical evidence supporting the impact of these practices in the WBs can be detected by public opinion polls, which show an overall positive view of China in WB states, unlike in EU countries. Chinese disinformation campaigns utilize a variety of tools, such as media outlets, social networks and propaganda-driven international news to improve China's image abroad. Additionally, Beijing has threatened the WB's institutional and political democratic resilience via hybrid mechanisms connected to cybersecurity vulnerability. Chinese propaganda strategy in the WBs is aimed at spreading an anti-Western narrative to slow down EU regional integration and Euro-Atlantic enlargement, while increasing Beijing's commercial, strategic, and diplomatic assets, and introducing an alternative political-economic model to the West pivoting on the "Beijing consensus".

China's rise in the Western Balkans and the technological quandary

Over the past years, particularly since 2008 – the year of the financial crisis in the EU – non-Western actors, including China, Russia, and Turkey, have [gained increasing influence](#) in the Western Balkans (WBs). Regarding China, its influence has been expanding significantly in the region as part of Beijing's geoeconomic and diplomatic vision of the Belt and Road Initiative (BRI) and the broader strategic context of China-EU relations. Several factors contributed to the increased Chinese engagement, [including](#) the stale of the Berlin Process regarding EU enlargement, existing development gaps, political affinity with undemocratic regimes in the region, and persistent governance, rule of law and corruption challenges. Indeed, since the beginning of the 2010s China has steadily expanded its regional influence mainly through investments and infrastructure projects, thereby increasing its economic and political assets. Furthermore, China promoted its role through media channels, cultural centres, NGOs, think tanks, governmental exchanges, student programmes, language schools, and cultural diplomacy. Also, a key tool in promoting Chinese engagement with the WBs has been the so-called [Cooperation between China and Central and Eastern European Countries](#) (China-CEE, China-CEEC, also 14+1; formerly 17+1 from 2019 to 2021 and 16+1 from 2012 to 2022) launched in 2012 to foster business and investment relations in the frame of the BRI.

Indeed, technology has been one of the key sectors in which Chinese influence has increased. In this sense, the [European Commission](#) has outspokenly described China as “an economic competitor in pursuit of technological leadership, and a systemic rival promoting alternative models of governance”. The issue of technology is closely linked to China's so-called [Three Warfare's Doctrine](#), which defines interstate conflict through three principles: legal warfare (the use of international law to advance strategic objectives), media warfare (the use of technology to shape public and international opinion) and psychological warfare (the use of manipulation of information to influence adversary decision-making and behaviour). In December 2003, the Chinese Communist Party's Central Committee (CCP) and Central Military Commission [approved](#) the doctrine to guide PLA political and information operations. Typically, China has been using technology both as a tool of sharp power for disinformation and propaganda purposes and as asymmetric mechanisms linked to cybersecurity vulnerabilities. Through hybrid warfare measures like the dissemination of disinformation and the launch of cyberattacks, China can coerce democratic societies, exploit their social, economic, and political divisions, and co-opt other states and their foreign policies by encouraging frozen conflicts, weaponizing political corruption, and restricting economic development in contested areas. Cyberattacks by China can negatively affect government agencies, global corporations, and small businesses, either directly or through cascading risks. Typically, cyberattacks manifest as unauthorized actions against computer infrastructure that compromise the confidentiality, integrity, or availability of its content. They [can bring about](#) financial losses, identity theft, distributed denial-of-service (DDoS),

phishing, spoofing, malwares, code injection attacks, supply chain attacks, social engineering attacks, insider threats, domain name system (DNS) tunnelling, IoT-based attacks, and AI-powered attacks. To be sure, due to their structural weaknesses – including underdeveloped levels of rule of law, civil society, and democratic governance, as well as chronicle instability and corruption –, the WBs provide fertile ground for undemocratic actors like Russia and China to manipulate and exploit governments and societies through [hybrid war measures](#), including cyberattacks, cyber intrusions, disinformation and fake news. Specifically, propagandistic strategies supported by malign cyberactivity aims at spreading an anti-Western narrative are easily assimilable in post-Yugoslav countries, particularly Serbia.

Thus, in the WBs technological quandaries and digital dilemmas are intertwined with geopolitical competition. Chinese sharp power and cyberactivity practices, could contribute to disrupting and undermining Euro-Atlantic integration, while increasing Beijing's commercial, strategic, and diplomatic assets, and introducing an alternative political-economic model to the West pivoting on the "Beijing consensus" - especially in relation to the current Berlin Process stalemate regarding EU enlargement in the region.

China's use of sharp power and technology as asymmetric threats in the Western Balkans

China's official discourse has been using the term "[soft power](#)" since 2007. Chinese soft power is closely linked to cultural diplomacy and is aimed at creating a feeling of [allure towards China](#), particularly in developing countries. However, Chinese soft power often evolved into [sharp power](#). From a notional perspective, "sharp power" represents a corrupted form of soft power - i.e., the ability to [co-opt through appeal and attraction rather than coercion](#). [Sharp power](#) is typical of authoritarian regimes, emphasising the use of propaganda, censorship, disinformation or manipulation to erode the integrity of independent institutions and seeking to limit free expression, spread confusion, and alter the political environment within democracies. [Sharp power practices](#) include:

- 1) Disguising malign initiatives as educational programmes, commercial ventures, or media endeavours;
- 2) Using proxy and intermediary networks to influence public discourse;
- 3) Interfering with elections; fomenting discord;
- 4) Using digital media platforms and digital tools to spread falsehoods.

Thus, a [sharp power strategy](#) involves coercive political actions that imitate soft power elements in order to influence a country's image, undermine its socio-political system, or force its government to take specific actions. Indeed, the Chinese Communist Party (CCP) has long recognised the value of [external promotion](#) under the label of

“dawaixuan” (大外宣), especially to shape a worldwide Sinophile narrative, marginalise dissenting voices, and securing a constituency of emotional, practical, and ideological support.

A key component of sharp power is represented by disinformation. The dissemination of disinformation poses a security threat as it exploits and disrupts the regular functioning of government and economic systems. [Disinformation](#) consists of lies sustained by false narratives often based on aggrievement and victimhood, which are used to manipulate people into believing what hostile and malignant disseminators know to be false. Similarly to cyberattacks on private and government networks, disinformation campaigns and the dissemination of fake news through social media outlets - including remarkably TikTok - or state-controlled media outlets serve as instruments of geopolitical power used by hostile and maligned actors to undermine institutions. To spread disinformation throughout Europe, the CCP has directly or indirectly set up hundreds - or perhaps thousands - of influencing networks, including Chinese-language newspapers, websites, apps, WeChat channels, foreign language newspaper inserts and advertisements, sponsored columns, education and business linkups, think tanks, films, TV news, talk shows, and documentaries. For instance, almost [100 Chinese-language media outlets](#) have been detected as pro-CCP throughout Europe.

Sharp power represents one aspect of the broader concept of hybrid warfare. In hybrid warfare, disinformation, cyberattacks, influence operations, and narratives of victimhood are used to create pretexts for conflict, promote discord, and maintain frozen conflict. A hybrid warfare strategy gives maligned powers the ability to exploit divisions, weaken resilience, and promote their interests and narratives. In hybrid warfare scenarios, cybersecurity represents a key target. [Cybersecurity indicators](#) tend to assess the levels of vulnerability of countries that are subject to malicious cyberactivity - including cyberattacks and cyber-intrusions. In the case of China, cybersecurity is often linked to the expansion of its 5G network.

In this frame, the WBs are especially vulnerable to actors seeking to damage infrastructure and create polarisation, given the specific local political, economic, and social conditions characterised by the lack of independent media and weak institutions and norms that allow the spread of disinformation. In the WBs hybrid warfare refers to a set of low-cost actions or tactics used to undermine public trust in institutions, weaken norms, and usually obstruct Euro-Atlantic integration. Also, in the WBs cybersecurity vulnerabilities are associated with hybrid war actions perpetrated by hostile forces, particularly cyberattacks and cyber-intrusions, along with disinformation campaigns. In the cybersecurity domain, one of the most significant challenges is the lack of local qualified experts in computer science, data science, and digitization, especially in the fields of national security and economic development. In the case of Russia or China, these countries use [proxies](#) to undermine the influence of the EU, NATO, and the US in the region, as well as promote social disorder and civilisational clash. In this frame, government leaders, judges, politicians, and citizens are

routinely targeted with fake news and falsehoods to undermine their pro-Western inclinations. For instance, Beijing is actively promoting disinformation through social, academic, and educational avenues, as well as through local political outlets, to enhance its influence through economic, energy, and infrastructure projects - including the 16+1 initiative.

China’s activities in the WB6

China’s increasing influence in the WB region has had consequences for all six non-EU WB countries – or Western Balkan Six (WB6) –, which comprise Albania, Bosnia-Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia. The footprint of China was visible in several areas, including technology, commercial, investment, and infrastructure. Nonetheless, recent analyses suggest that China’s *disinformation* is still more a hype than a reality at present, with Russia remaining the main tangible source of disinformation in the WBs. Recent research based on media analyses and public opinion indicates that *China’s appeal may be growing*, but its influence may not be as great as often claimed – including in places such as Serbia. Additionally, a recent study about China’s disinformation suggests that Western narratives tend to overemphasize the role of technology and sophisticated software, while overlooking the fact that much of China’s digital authoritarianism still relies on extensive human intelligence: such reliance on human input might explain why *China’s disinformation* is more nuanced and sophisticated in places such as Taiwan or Southeast Asia than in Europe. Still, data from public opinion polls provides insight into the effectiveness and spread of Chinese disinformation in the WBs – highlighting public opinion shifts in favour of Beijing in the past decade. For instance, as summarized in Table 1, a survey in post-Yugoslav Balkan countries (thus, omitting Albania) detected that in 2020 the public perceptions on China in the WBs were *mainly favourable*.

Western Balkan country	Favourable view of China (in %)	Unfavourable view of China (in %)
Bosnia-Herzegovina	52	37
North Macedonia	56	35
Montenegro	68	22
Serbia	85	11

Table 1: Western Balkan countries’ view on China in 2020. Source: https://www.iri.org/wp-content/uploads/2020/06/final_wb_poll_for_publishing_6.9.2020.pdf.

Compared to the average EU country perception on China, which, as shown in Table 2, is definitely unfavourable, in the WBs this trend is therefore reverted.

EU country	Favourable view of China (in %)	Unfavourable view of China (in %)
France	23	70
Germany	20	76
Italy	35	61
Netherlands	22	74
Poland	18	71
Spain	33	55

Table 2: EU countries' view on China in 2024. Source: <https://www.startista.com/statistics/921671/euro-pean-perception-of-china-by-country/>.

The comparison of public opinion's perception in EU and WB countries respectively adds empirical evidence on the effectiveness of Chinese soft/sharp power, demonstrating how Beijing was able to build a positive image of itself in the WB region, which, unlike the EU, is more liable to foreign influence intrusions.

Albania

In the technological domain, in 2019 Albanian public radio and television signed a cooperation agreement with the Chinese counterpart, endorsing the broadcast of Chinese documentaries, including films about President Xi Jinping, as well as other cultural and economic programs. Also, Beijing sends cartoons to major media channels in the country to promote communication and distribute content targeted at younger audiences. It is primarily through "Ejani Radio" - essentially a branch of China Radio International (CRI) which also enjoys a YouTube channel and a Facebook page - that information about China is distributed. Overall, the [presence of China-related content](#) across the media spectrum in the country is evident, with a constant rise between 2014 and 2019 in contents related to the BRI.

Bosnia-Herzegovina

As for Bosnia-Herzegovina, China wishes to enhance its role in the country even through Huawei 5G technologies and several events linked to the BRI. In the case of the media, "Xinhua" news agency created institutional links via cooperation agreements with the "Federal News Agency" (FENA), "Radio and Television of Bosnia-Herzegovina" (BHRT), and "Patria" News Agency, as well as with "Republika Srpska News Agency". In addition, Sarajevo and Beijing signed a cooperation memorandum in 2019 that envisages exchange visits, content sharing, joint news coverage, as well as joint activities in publishing, broadcasting, and film production. Finally, the website "China Today" and the magazine "Voice of China" contribute to spreading China's influence in the country.

Montenegro

In relation to Montenegro, in the field of the media there has been a steady flow of pro-Chinese content being broadcast via Serbian news. Also, some Montenegrin pro-Chinese (and pro-Russian) websites comprise [www.in4s.net](#) and [borba.me](#). For example, [borba.me](#) frequently refers to China in an apologetic manner in its news reports, manifesting a [biased pro-Chinese inclination](#) and espousing [Beijing's rhetoric](#) vis-à-vis the West, NATO, and the US.

North Macedonia

As for North Macedonia – a country [particularly vulnerable](#) to non-western intrusions –, in terms of the media, cooperation agreements between North Macedonia and China date back to 2004 and involve content sharing, exchange visits and material support. China-friendly contents – often devoid of any critical analysis and characterised by unclear sources, half-truths, unverified data, speculative assumptions, and disinformation – are [broadcasted by](#) TV channels like “Kanal 5” and “Sitel TV”, news agencies such as “MakFax” and the internet portals “Republika” and “Kurir”.

Serbia (and Kosovo)

Finally, in relation to Serbia – and incidentally Kosovo, since China does not recognize its independence –, China views the country as its chief strategic partner in the WBs. In turn, Serbia considers China its [second most important ally](#) after Russia. In Serbia, Chinese investments include the [Safe City Project](#) in which Chinese high-tech companies, including Huawei, have installed 1,000 CCTV cameras in 800 secret locations throughout Belgrade. Since this technology is equipped with facial recognition software and the capacity to identify license plates, it is considered threatening because the Chinese companies involved are required under the Chinese National Security Act to relay all data in their possession to [Beijing's intelligence service](#). Also, these facial recognition cameras were unlawfully used by the Serbian police to film and later identify protesters who demonstrated against the low environmental standards of a lithium mine in the country. Generally, the [Serbian market](#) has been one of Huawei's most important regional markets – also through important agreements signed between Huawei and Serbian Telecom for the digitalisation of Serbia. Also, since 2006 Confucius Institutes have been operating in Serbia, spreading the Chinese language and culture among Serbian pupils and students and enhancing a full-fledged strategy that pivots on [cultural diplomacy](#). Moreover, Chinese funding is also directed at Serbian think tanks, which are geopolitically oriented and perceived as pro-Chinese and as potential academic multipliers. In the sphere of media cooperation, Beijing and Belgrade signed a series of agreements. Consistently, in recent years there has been an increase in the number of stories related to China in the Serbian media, which generally depict China in a very positive way. Some pro-Chinese outlets include “China Radio International”,

“China Today” (“Kina Danas”), “Informer”, and “Welcome to Fun Radio”. Finally, the Chinese technology giant Huawei is a major player on the Serbian media advertising market, further solidifying Chinese dominance within the wider public sphere.



This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which these article have been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent. Deed - Attribution 4.0 International - Creative Commons

This EuroHub4Sino Policy Paper contains links to external third-party websites. These links to third-party sites do not imply approval of their contents. EuroHub4Sino has no influence on the current or future contents of these sites. We therefore accept no liability for the accessibility or contents of such websites and no liability for damages that may arise as a result of the use of such content.



Funded by
the European Union

The project "European Hub for Contemporary China (EuroHub4Sino)" has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement number 101131737.

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.